

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

[Signature]

П.А. Машаров

«29» марта 2024 г.
МП

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ
КАНАЛАМ»

Укрупненная 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 «**Защита информации от утечки по техническим каналам**» 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

 М.В. Бабичева

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:

Электротехника, Электроника и схемотехника, Сети и системы передачи информации, Программно-аппаратные средства защиты информации, Аппаратные средства вычислительной техники, Основы информационной безопасности, Методы и средства криптографической защиты информации, Архитектура и администрирование операционных систем.

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

Основы управления информационной безопасностью, Цифровые системы обработки информации, Оптоэлектронные датчики.

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 Защита информации от утечки по техническим каналам
Часть образовательной программы	Базовая часть (профессионально-ориентированные дисциплины)
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	4	7	30	30	-	84	144	экзамен

3. ЦЕЛИ ДИСЦИПЛИНЫ

Изучить современное представление о видах, источниках и носителях защищаемой информации, дать классификацию и основные характеристики технических каналов утечки информации и методов инженерно-технической защиты информации, представить государственную систему противодействия технической разведке, виды контроля эффективности защиты 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-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.2 Умеет применять средства технической защиты информации для решения задач профессиональной деятельности	Знает основные принципы построения средств технической защиты информации для решения задач профессиональной деятельности. Умеет использовать средства технической защиты информации для решения задач профессиональной деятельности
ОПК-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности аппаратных средств защиты информации автоматизированных систем	Знает основные физические законы, связанные с распространением, поглощением и отражением звуковых и радиоволн, а также генерацией шум подобных сигналов. Умеет выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности аппаратных средств защиты информации автоматизированных систем
ОПК-17 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-17.1 Умеет проводить диагностику и мониторинг средств технической защиты информации для автоматизированных систем	Владеет навыками и методиками применения средств технической защиты информации для решения задач профессиональной деятельности

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
1. Структура и основные характеристики технических каналов утечки информации.	<ol style="list-style-type: none"> 1. Правовые основы технической защиты информации. 2. Классификация каналов технической разведки. 3. Краткая характеристика каждого канала. 4. Возможности различных видов технической разведки. Историческая справка. 5. Параметрический канал утечки, исторические примеры. 6. Демаскирующие признаки объектов наблюдения и сигналов. 7. Опасные сигналы и их источники. 8. Физические процессы, приводящие к появлению побочных излучений и формированию технических каналов утечки информации.
2. Радиозакладные устройства.	<ol style="list-style-type: none"> 1. Принципы работы радиозакладных устройств. 2. Обнаружение и локализация закладных устройств. 3. Методы поиска закладных устройств. 4. Использование эффекта нелинейного рассеяния ЭМ для обнаружения и локализации закладных устройств. 5. Детекторы РЗУ.

3. Утечка по акустическому каналу.	1. Акустический канал утечки информации. 2. Физические процессы, приводящие к появлению опасных акустических сигналов. 3. Характеристики побочных акустических сигналов. 4. Типы микрофонов. 5. Направленные микрофоны. 6. Методы борьбы с утечкой по акустическому каналу.
4. Подавители сигналов.	1. Акустический шум. 2. Виды шума. Белый шум. 3. Уровни шума. 4. Спектральные уровни шума. 5. Речевые помехи. 6. Генераторы акустического шума. 7. Генераторы речеподобных помех. 8. Скремблеры. 9. Постановщики радиопомех.
5. Утечка по виброканалу.	1. Вибрационный канал утечки информации. 2. Физические процессы, приводящие к появлению опасных вибросигналов. 3. Характеристики вибрационных сигналов. 4. Стетоскопы и вибродатчики. 5. Особенности строительных конструкций и возможность утечки. 6. Методы борьбы с утечкой по виброканалу.
6. Утечка по оптическому каналу.	1. Основные возможности утечки по оптическому каналу. 2. Удаленный обзор, бинокли. 3. Приборы ночного видения. 4. Лазерные прослушивающие устройства. 5. Видеонаблюдение, как канал утечки и метод защиты. Видеокамеры и видеомониторы.
7. Защита мобильной связи.	1. Программные и аппаратные средства прослушки. 2. Шпионские программы 3. Вирусы для мобильных систем. 4. Предоставление данных оператором 5. Перехват сообщений между станцией и телефоном. 6. Физические основы и технические решения перехвата мобильных сообщений. 7. ISM ловушки и специальная аппаратура для перехвата. 8. Акустические сейфы и другая аппаратная защита мобильных телефонов.
8. Защита компьютеров и компьютерных сетей.	1. Формирование каналов утечки информации за счёт наводок на посторонние проводники, случайные антенны, цепи питания и заземления. 2. Основные характеристики технических каналов утечки информации образованных за счёт наводок. 3. Уязвимости в сетях. 4. Защита IP адресов. 5. Защита жестких дисков и съемных носителей. 6. Защита ВОЛС.
9. Системы аутентификации и	1. Ограничение доступа. 2. Технические и биометрические системы аутентификации.

охранные системы.	3. Охранные системы. 4. Датчики для охранных систем. 5. Системы сигнализации. 6. Системы охраны периметра.
-------------------	---

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – очная, курс – 1, семестр – 1

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор	Практ.	СРС+К	Всего
Структура и основные характеристики технических каналов утечки информации.	4	4		6	14
Радиозакладные устройства.	4	4		6	14
Утечка по акустическому каналу.	4	4		6	14
Подавители сигналов.	4	4		6	14
Утечка по виброканалу.	4	4		6	14
Утечка по оптическому каналу.	4	4		6	14
Защита мобильной связи.	4	4		6	14
Защита компьютеров и компьютерных сетей.	4	4		8	16
Системы аутентификации и охранные системы.	2	2		8	12
ИТОГО ЗА СЕМЕСТР / ЗА КУРС / ПО КОМПОНЕНТУ ОПОП	34	34		54,1+3,9	126
ИТОГО ПО КОМПОНЕНТУ ОПОП	34	34		58	126

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

7.1. Контрольные вопросы

1. Правовые основы технической защиты информации.
2. Что такое техническая защита информации. Где применяется, с чем имеет дело.
3. Что такое канал утечки информации. Приведите примеры.
4. Какие каналы утечки информации вы знаете.
5. Технические каналы утечки речевой информации.
6. Прямой акустический канал. Структура канала. Все, что вы знаете о звуке.
7. Уровни слышимости звуковой информации. Порог слышимости. В каких единицах измеряется уровень слышимости.
8. Акустоэлектромагнитный канал утечки информации.
9. Виброакустический канал утечки информации.
10. Параметрический канал утечки информации.
11. Оптические каналы утечки информации.
12. Технические каналы утечки информации, обрабатываемой ТСМИ.
13. Что такое РЗУ. Из каких частей они состоят чаще всего.
14. Пассивные, полуактивные и активные РЗУ.
15. Какие генераторы несущей для РЗУ вы знаете? От чего зависит частота генерируемого сигнала?
16. Каким образом происходит модуляция несущей в РЗУ?
17. Классификация РЗУ
18. Частотные диапазоны, в которых работают РЗУ.
19. Виды модуляции, применяемые для РЗУ.
20. Что такое VOX (акустомат) и для чего он нужен.
21. Какими параметрами определяется дальность действия РЗУ?

22. Методы выявления РЗУ.
23. Методы поиска ЗУ, как физических объектов.
24. Методы поиска ЗУ, как электронных устройств.
25. Что такое детектирование сигнала?
26. Чем отличается приемник прямого усиления и супергетеродинный приемник?
27. Из каких частей состоит простой детекторный приемник?
28. Что такое SDR-приемник? Принцип работы, частоты, какие функции можно перестраивать.

7. 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 Информационная безопасность *

Форма обучения Очная

Семестр Седьмой

Дисциплина Защита информации от утечки по техническим

каналам

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Виброакустический технический канал утечки речевой информации. Структура канала. Что такое пьезоэлектрический эффект и какова его роль в виброрадиозакладных устройствах.
2. Угрозы в компьютерных сетях и методы борьбы с ними
3. Аналоговые и цифровые источники шума. Преимущества и недостатки аналоговых и цифровых источников шума. Речеподобная помеха и ее роль в защите акустического канала.
4. Что такое детектирование сигнала? Чем отличается приемник прямого усиления и супергетеродинный приемник? Из каких частей состоит простой детекторный приемник?
5. Снятие информации с оконного стекла. Физические принципы и схема установки.

Утверждено на
заседании кафедры.

Зав. кафедрой РФ и
ИКТ

В.В. Данилов

№ _____ от
_____ 202_г.

Экзаменатор

М.В.Бабичева

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
	Контрольная работа	10
	Лабораторные работы	30
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 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. Ленков, С. В. Методы и средства защиты информации [Текст] : в 2 т. Т. 1 : Несанкционированное получение информации / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. - Киев : Арий, 2008. - 464 с.
2. Ленков, С. В. Методы и средства защиты информации [Текст] : в 2 т. Т. 2 : Информационная безопасность / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. - Киев : Арий, 2008. - 342 с.
3. Хотунцев, Ю. Л. Основы радиоэлектроники : Учеб. пособие для студентов физ. и технол.-экон. фак. / Ю. Л. Хотунцев, А. Лобарев. - М. : АГАР, 1998. - 284 с.
4. 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.

11.2. Дополнительная литература

5. Федеральный закон об информации, информатизации и защите информации : Коммент. / И. Л. Бачило, А. В. Волокитин, М. Л. Колчинский и др. ; Ком. при президенте РФ по политике информатизации ; Ин-т государства и права РАН ; Науч.-техн. центр "Информсистема". - М. : Ин-т государства и права РАН, 1996. - 83

6. Лапони́на, О. Р. Межсетевое экранирование : учеб. пособие / О. Р. Лапони́на. - М. : Интернет-ун-т информ. технологий : Бином. Лаб. знаний, 2007. - 343 с.

12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Общие вопросы технической защиты информации . – URL: <https://www.intuit.ru/studies/courses/2291/591/lecture/12677>). – Режим доступа: свободный

2. Техническая защита информации . – URL: <http://confident.org.ua/index.php/stati-po-teme/170-tekhnicheskaya-zashchita-informatsii.html>). – Режим доступа: свободный

3. Техническая защита информации в автоматизированных системах управления производственными и технологическими процессами . – URL: https://www.infosystems.ru/courses/kursy_soglasovannye_s_federalnymi_organami/tekhnicheskaya_zashchita_informatsii_v_avtomatizirovannykh_sistemakh_upravleniya_proizvodstvennymi_i/). – Режим доступа: свободный

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

5. 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

6. Интернет-библиотека Виталия Арнольда URL: <http://ilib.mccme.ru/> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный;

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

8. 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)