

УТВЕРЖДАЮ
 Декан факультета

_____ Страхов С.Ю.

«___» _____ 20__

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ РАДИОЭЛЕКТРОННАЯ ЗАЩИТА ОБЪЕКТОВ И ИНФОРМАЦИИ

Направление/специальность подготовки	09.03.02 Информационные системы и технологии
Специализация/профиль/программа подготовки	Информационная безопасность
Уровень высшего образования	Бакалавриат
Форма обучения	Очная
Факультет	О Естественнонаучный
Выпускающая кафедра	О7 Информационные системы и программная инженерия
Кафедра-разработчик рабочей программы	И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

КУРС	СЕМЕСТР	ОБЩАЯ ТРУДОЁМКОСТЬ (ЗАЧЕТНЫХ ЕДИНИЦ)	ЧАСЫ (по наличию видов занятий)									ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
			ОБЩАЯ ТРУДОЁМКОСТЬ	АУДИТОРНЫЕ ЗАНЯТИЯ				САМОСТОЯТЕЛЬНАЯ РАБОТА				
				ВСЕГО	ЛЕКЦИИ	ЛАБОРАТОРНЫЙ ПРАКТИКУМ	ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	ВСЕГО	КУРСОВОЙ ПРОЕКТ	КУРСОВАЯ РАБОТА	ДРУГИЕ ВИДЫ САМОСТ. РАБОТЫ	
3	5	3	108	51	34	0	17	57	0	0	57	диф. зач.

ЛИСТ СОГЛАСОВАНИЯ

РАБОЧАЯ ПРОГРАММА СОСТАВЛЕНА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЕДЕРАЛЬНОГО
ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)

09.03.02 Информационные системы и технологии

год набора группы: 2025

Программу составил:

Кафедра И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ
Стукалова Анна Сергеевна, старший преподаватель

Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы **И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ**

Заведующий кафедрой Страхов С.Ю., д.т.н., проф.

Программа рассмотрена
на заседании выпускающей кафедры

О7 Информационные системы и программная инженерия

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

РАДИОЭЛЕКТРОННАЯ ЗАЩИТА ОБЪЕКТОВ И ИНФОРМАЦИИ

Разделы рабочей программы

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО
3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приложения к рабочей программе дисциплины

- Приложение 1. Аннотация рабочей программы
- Приложение 2. Технологии и формы обучения
- Приложение 3. Фонды оценочных средств

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ПК-2.3 — Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

Формированию компетенций служит достижение следующих результатов образования:

ПК-2.3

знания:

знать современные информационные технологии и основные подходы к защите информации;

знать принципы радиоэлектронной защиты объектов и информации;

умения:

уметь оценивать защищенность информации;

уметь применять различные преобразования для решения задач обеспечения защиты информации;

навыки:

уметь оценивать обстановку и применять методы защиты информации от технических разведок и от ее утечки по техническим каналам.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **РАДИОЭЛЕКТРОННАЯ ЗАЩИТА ОБЪЕКТОВ И ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*.

Содержание дисциплины является логическим продолжением дисциплин: **ФИЗИЧЕСКИЕ ОСНОВЫ МИКРОЭЛЕКТРОНИКИ, СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**.

Содержание дисциплины является основой для освоения дисциплин: **ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-1 — Способен применять естественнонаучные и общетехнические знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности
- ОПК-2 — Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности
- ОПК-5 — Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем
- ОПК-7 — Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

3.1. Содержание (дидактика) дисциплины

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %
				ВСЕГО	Лекции	Практические занятия		ПК-2.3
3	5	Раздел 1. Принципы радиоэлектронной защиты объектов и информации. Методы криптографической защиты. Принципы кодового зашумления. Защита информации путем временных и спектральных преобразований сигнала. Принципы разграничения доступа к информации. Способы обнаружения несанкционированного доступа к объекту. Пути реализации защиты от утечек за счет побочных излучений и наводок. Защита протяженных линий телекоммуникаций. Защита компьютеров и вычислительных сетей. Защита информации от случайных воздействий.	52	24	16	8	28	50
3	5	Раздел 2. Технические средства радиоэлектронной защиты. Датчики. Кодеры и скремблеры. Генераторы шума и аппаратура шумочистки. Радиоприемники и радиопередатчики специального назначения. Нелинейные локаторы. Аппаратура контроля доступа.	56	27	18	9	29	50
Всего за 5 семестр			108	51	34	17	57	100
Всего по дисциплине			108	51	34	17	57	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Принципы радиоэлектронной защиты объектов и информации.	Отработка тематик раздела	8
2	Раздел 2. Технические средства радиоэлектронной защиты.	Отработка тематик раздела	9
Всего за 5 семестр			17

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Принципы радиоэлектронной защиты объектов и информации.	Изучение дидактических единиц раздела	28
2	Раздел 2. Технические средства радиоэлектронной защиты.	Изучение дидактических единиц раздела	29
Всего за 5 семестр			57

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	НЕДЕЛИ СЕМЕСТРА																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
5		ИПЗ		ТекК	ИПЗ	ДР	ИПЗ	ТекК	ИПЗ	ДР		ТекК	ИПЗ		ТекК	ДР	диф. зач.

Условные обозначения:

- ДР – диагностическая работа;
- ТекК – вопросы для текущего контроля;
- ИПЗ – индивидуальное практическое задание;
- диф. зач. – дифференцированный зачет.

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- вопросы для текущего контроля;
- индивидуальное практическое задание.

- Промежуточная аттестация** проводится в формах:
- дифференцированный зачет.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. А. А. Внуков. . Защита информации. Москва: Юрайт, 2021, эл. рес.
2. Л. Б. Кочин. . Средства радиоэлектронной защиты. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008, эл. рес.

5.2. Дополнительная литература по дисциплине:

не требуется.

5.3. Периодические издания:

не требуются.

5.4. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины, электронные библиотечные системы:

не требуется.

Современные профессиональные базы данных:

1. <https://rusneb.ru> – Национальная электронная библиотека (НЭБ);
2. <https://cyberleninka.ru/> - Научная электронная библиотека «Киберленинка»;
<http://www.rfbr.ru/rffi/ru/library> - Полнотекстовая электронная библиотека Российского фонда фундаментальных исследований.

Информационные справочные системы:

1. Техэксперт – Информационный портал технического регулирования: Нормы, правила, стандарты РФ;
2. http://library.voenmeh.ru/jirbis2/index.php?option=com_irbis&view=irbis&Itemid=457 - БД ГОСТов собственной генерации БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова;
3. <http://www.consultant.ru/>- КонсультантПлюс- информационный портал правовой информации.

5.5. Программное обеспечение:

1. MATLAB R 2015a.

5.6. Информационные технологии:

взаимодействие с обучающимися посредством ЭИОС Moodle БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Лекционные занятия:

специализированные требования по оборудованию отсутствуют; аудитория с посадочными местами по количеству студентов; доска.

6.2. Практические занятия:

1. Проектор;
2. MATLAB R 2015a.

6.3. Прочее:

1. рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
2. рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

Аннотация рабочей программы

Дисциплина **РАДИОЭЛЕКТРОННАЯ ЗАЩИТА ОБЪЕКТОВ И ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*. Дисциплина реализуется на факультете *И Информационных и управляющих систем* БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой **И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ**.

Дисциплина нацелена на формирование *компетенций*:

ПК-2.3 Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

Содержание дисциплины охватывает круг вопросов, связанных с принципами радиоэлектронной защиты объектов и информации, а также с техническими средствами радиоэлектронной защиты.

Программой дисциплины предусмотрены следующие **виды контроля**:

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- вопросы для текущего контроля;
- индивидуальное практическое задание.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

Общая трудоемкость освоения дисциплины составляет **3 з.е., 108 ч.** Программой дисциплины предусмотрены лекционные занятия (**34 ч.**), практические занятия (**17 ч.**), самостоятельная работа студента (**57 ч.**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 51 ч. аудиторных занятий, и 57 ч., отведенных на самостоятельную работу студента.

Рекомендации по распределению учебного времени по видам самостоятельной работы и разделам дисциплины приведены в таблице.

Контроль освоения дисциплины производится в соответствии с Положением о текущем, рубежном контроле успеваемости и промежуточной аттестации обучающихся.

Формы контроля и критерии оценивания приведены в приложении 3 к Рабочей программе.

Наименование работы	Рекомендуемая литература	Трудоемкость, час.
Раздел 1. Принципы радиоэлектронной защиты объектов и информации.		
Изучение дидактических единиц раздела	Л. Б. Кочин. . Средства радиоэлектронной защиты: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008 (1.1-1.10) А. А. Внуков. . Защита информации: Москва: Юрайт, 2021 (1,2,3)	28
Итого по разделу 1		28
Раздел 2. Технические средства радиоэлектронной защиты.		
Изучение дидактических единиц раздела	Л. Б. Кочин. . Средства радиоэлектронной защиты: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008 (2.1-2.10)	29
Итого по разделу 2		29

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств, позволяющие оценить результаты обучения по данной дисциплине, включают в себя:

- диагностическая работа
- вопросы для текущего контроля;
- индивидуальное практическое задание;
- дифференцированный зачет.

Критерии оценивания

Диагностическая работа

Диагностическая работа проводится в форме теста в ЭИОС Moodle:

- при правильном ответе менее чем на 60% вопросов - не аттестация;
- при правильном ответе на 60% вопросов и более - аттестация.

Вопросы для текущего контроля

Тест включает в себя 10 вопросов. Требуется выбирать один правильный ответ из предложенных. Время выполнения 10 минут. Успешное прохождение теста регистрируется при условии получения не менее 6 правильных ответов. Оценка "хорошо" - не менее 8 правильных ответов. Оценка "отлично" - не менее 9 правильных ответов.

Примеры представлены в УМК в дисциплины.

Индивидуальное практическое задание

Отчет по индивидуальному заданию должен содержать полное решение согласованной с преподавателем задачи.

Дифференцированный зачет

Итоговый контроль по дисциплине проходит в форме дифференцированного зачета, который выставляется на 17 неделе семестра. Оценка выставляется как среднее арифметическое оценок за тесты.

Паспорт фонда оценочных средств

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %	НАИМЕНОВАНИЕ ОЦЕНОЧНОГО СРЕДСТВА
				ВСЕГО	Лекции	Практические занятия		ПК-2.3	
3	5	Раздел 1. Принципы радиоэлектронной защиты объектов и информации.	52	24	16	8	28	50	Вопросы для текущего контроля, Индивидуальное практическое задание
3	5	Раздел 2. Технические средства радиоэлектронной защиты.	56	27	18	9	29	50	Вопросы для текущего контроля, Индивидуальное практическое задание
Всего за 5 семестр			108	51	34	17	57	100	
Всего по дисциплине			108	51	34	17	57	100	

Оценочные материалы по дисциплине РАДИОЭЛЕКТРОННАЯ ЗАЩИТА ОБЪЕКТОВ И ИНФОРМАЦИИ

ПК-2.3 - Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

№ 1 Прочитайте текст и запишите развернутый обоснованный ответ

Под информационной безопасностью понимается:

№ 2 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Ответьте и обоснуйте:

Утечка информации – это ...

- процесс раскрытия секретной информации
- несанкционированный процесс переноса информации от источника к злоумышленнику
- процесс уничтожения информации
- непреднамеренная утрата носителя информации

№ 3 Прочитайте текст и запишите развернутый обоснованный ответ

Защита информации – это ...

№ 4 Прочитайте текст и установите соответствие

Сопоставьте способ наблюдения и техническое средство:

1. визуально-оптический;

2. с помощью приборов наблюдения в ИК-диапазоне;

3. акустический;

А. тепловизор

Б. камера

В. микрофон

№ 5 Прочитайте текст и установите соответствие

1. Спуфинг

2. Джемминг

3. Взлом

А. Подмена

Б. Глушение

В. Удачная криптоатака

№ 6 Прочитайте текст и установите последовательность

Установите последовательность действий во времени:

1. Идентификация

2. Аутентификация

3. Авторизация

4. Работа в системе

№ 7 Прочитайте текст и установите последовательность

Установите последовательность модели от нижнего уровня к верхнему

1. Физический уровень
2. Прикладной уровень
3. Уровень представления
4. Сеансовый уровень
5. Транспортный уровень
6. Сетевой уровень
7. Канальный уровень

№ 8 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Ответьте и обоснуйте:

Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ):

МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты

МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения

№ 9 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Ответьте и обоснуйте:

Сервисы безопасности:

- контроль целостности
- кэширование записей
- регулирование конфликтов
- экранирование
- идентификация и аутентификация
- инверсия паролей
- обеспечение безопасного восстановления
- шифрование

№ 10 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Ответьте и обоснуйте:

Причины возникновения ошибки в данных

- Использование недопустимых методов анализа данных
- Преднамеренное искажение данных
- Ошибка при записи результатов измерений в промежуточный документ
- Неверная интерпретация данных
- Ошибки при переносе данных с промежуточного документа в компьютер
- Погрешность измерений
- Неустраняемые причины природного характера
- Ошибки при идентификации объекта или субъекта хозяйственной деятельности

№ 11 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Ответьте и обоснуйте:

Основные угрозы конфиденциальности информации:

- маскарад
- злоупотребления полномочиями

- блокирование
- перехват данных
- карнавал
- переадресовка

№ 12 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Ответьте и обоснуйте:

Информация, составляющая государственную тайну не может иметь гриф...

- «особой важности»
- «секретно»
- «совершенно секретно»
- «для служебного пользования»