

УТВЕРЖДАЮ
 Декан факультета

 (подпись) Страхов С. Ю.
 ФИО
 «___» _____ 20__

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление/специальность подготовки	12.03.03 Фотоника и оптоинформатика
Специализация/профиль/программа подготовки	Оптоинформационные системы
Уровень высшего образования	Бакалавриат
Форма обучения	Очная
Факультет	И Информационных и управляющих систем
Выпускающая кафедра	И1 ЛАЗЕРНАЯ ТЕХНИКА
Кафедра-разработчик рабочей программы	И1 ЛАЗЕРНАЯ ТЕХНИКА

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	
4	8	3	108	52	26	0	26	56	0	0	56	диф. зач.

ЛИСТ СОГЛАСОВАНИЯ

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

12.03.03 Фотоника и оптоинформатика

год набора группы: 2024

Программу составил:

Кафедра И1 ЛАЗЕРНАЯ ТЕХНИКА
Петрова Юлия Юрьевна, старший преподаватель

Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы **И1 ЛАЗЕРНАЯ ТЕХНИКА**

Заведующий кафедрой Борейшо А.С., д.т.н., проф.

Программа рассмотрена
на заседании выпускающей кафедры

И1 ЛАЗЕРНАЯ ТЕХНИКА

Заведующий кафедрой Борейшо А.С., д.т.н., проф.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ МЕТОДЫ ЗАЩИТЫ 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:

ПСК-2.1 — способность к анализу поставленной задачи исследований в области фотоники и оптоинформатики

Формированию компетенций служит достижение следующих результатов образования:

ПСК-2.1

знания:

на уровне представлений: физические принципы, используемые для получения, передачи, хранения, обработки и защиты информации;

на уровне воспроизведения: принципы построения систем защиты информации;

на уровне понимания: основы теории и принципы действия компонентов и устройств систем защиты информации;

умения:

теоретические: применять методы теории обработки и защиты информации;

практические: применять методы экспериментального исследования систем обработки и защиты информации и их функциональных узлов;

навыки:

владеть математическим аппаратом для решения теоретических и прикладных задач при моделировании и проектировании систем обработки и защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ** является дисциплиной **части**, формируемой участниками образовательных отношений блока 1, программы подготовки по направлению 12.03.03 *Фотоника и оптоинформатика*.

Содержание дисциплины является логическим продолжением дисциплин: **ТЕОРИЯ СИГНАЛОВ И СИСТЕМ, ЦИФРОВАЯ ОБРАБОТКА СИГНАЛОВ В ОПТОИНФОРМАЦИОННЫХ СИСТЕМАХ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ПСК-2.1 — Способен к анализу поставленной задачи исследований в области фотоники и оптоинформатики
- ПСК-2.4 — Способен определять требуемые параметры систем обработки сигналов и трактов передачи в зависимости от свойств источников и приемников информации

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		ПСК-2.1
4	8	Раздел 1. Понятия и определения дисциплины. 1.1. Информация как объект защиты. 1.2. Общие принципы защиты информации. 1.3. Обобщенная структурная схема системы защиты информации. 1.4. Особенности защиты информации в оптоинформационных системах.	4	2	2	0	2	10
4	8	Раздел 2. Общие сведения о криптографической защите информации. 2.1. Понятие криптографической защиты информации. 2.2. Классификация методов криптографической защиты. 2.3. Общие сведения о симметричных методах криптографической защиты. 2.4. Понятие о несимметричных методах криптографической защиты. 2.5. Требования к методам криптографической защиты.	6	4	4	0	2	10
4	8	Раздел 3. Симметричные криптографические системы. 3.1. Методы подстановки и перестановки. 3.2. Понятие гаммы. Метод гаммирования. 3.3. Метод Вижинера. 3.4. Комбинированные методы криптографической защиты информации. 3.5. Примеры симметричных криптографических систем.	14	8	4	4	6	12
4	8	Раздел 4. Несимметричные криптографические системы. 4.1. Понятие открытого и секретного ключа. 4.2. Виды несимметричных криптографических преобразований. 4.3. Несимметричные алгоритмы защиты информации. 4.4. Примеры реализации несимметричных криптографических систем.	12	6	2	4	6	12
4	8	Раздел 5. Основы криптографического анализа. 5.1. Понятия частотного распределения символов и индекса соответствия. 5.2. Криптографический анализ одноалфавитных и многоалфавитных шифровальных систем. 5.3. Особенности реализации криптоаналитических методов.	18	10	2	8	8	10
4	8	Раздел 6. Метод защиты информации на основе кодового зашумления. 6.1. Принцип кодового зашумления. 6.2. Структура основного и отводного канала. 6.3. Алгоритмы кодового зашумления. 6.4. Понятие о широкополосных и квантовых системах защиты информации.	8	2	2	0	6	12
4	8	Раздел 7. Защита информации на основе временных и спектральных преобразований сигналов. 7.1. Методы временных преобразований информационных сигналов. 7.2. Методы защиты на основе спектральных преобразований информационных сигналов. 7.3. Понятие скремблирования, кодеки и скремблеры. 7.4. Общие сведения о защите информации от несанкционированного доступа за счет побочных излучений и наводок. 7.5. Защита информации протяженных линиях телекоммуникаций.	18	10	4	6	8	12
4	8	Раздел 8. Защита информации путем разграничения доступа. 8.1. Методы контроля доступа к информации. 8.2. Понятия аутентификации и идентификации. 8.3. Дискретизационный и мандатный принципы разграничения доступа к информации. 8.4. Метод разделения привилегий.	4	2	2	0	2	10
4	8	Раздел 9. Защита информации в персональных компьютерах и вычислительных сетях. 9.1. Понятие потенциально опасных функций. Защищенное программирование. 9.2. Безопасность операционных систем. 9.3. Методы обнаружения несанкционированного доступа в компьютерах и вычислительных сетях. 9.4. Защита информации от случайных воздействий.	24	8	4	4	16	12
Всего за 8 семестр			108	52	26	26	56	100
Всего по дисциплине			108	52	26	26	56	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 3. Симметричные криптографические системы.	Изучение методов подстановки и перестановки, гаммирования	2
2		Защита информации с помощью таблиц Вижинера	2
3	Раздел 4. Несимметричные криптографические системы.	Комбинированные методы защиты информации	4
4		Контрольная работа 1	2
5	Раздел 5. Основы криптографического анализа.	Комбинированные методы защиты информации	6
6		Изучение методов скремблирования	4
7	Раздел 7. Защита информации на основе временных и спектральных преобразований сигналов.	Контрольная работа 2	2
8		Изучение методов обнаружения	4

компьютерах и вычислительных сетях.	НСД к информации	
Всего за 8 семестр		26

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Понятия и определения дисциплины.	Изучение предусмотренных программой дидактических единиц по конспектам лекций и рекомендуемой литературе	2
2	Раздел 2. Общие сведения о криптографической защите информации.	Изучение предусмотренных программой дидактических единиц по конспектам лекций и рекомендуемой литературе	2
3	Раздел 3. Симметричные криптографические системы.	Изучение предусмотренных программой дидактических единиц по конспектам лекций, материалам практических занятий и рекомендуемой литературе	6
4	Раздел 4. Несимметричные криптографические системы.	Изучение предусмотренных программой дидактических единиц по конспектам лекций, материалам практических занятий и рекомендуемой литературе	6
5	Раздел 5. Основы криптографического анализа.	Изучение предусмотренных программой дидактических единиц по конспектам лекций, материалам практических занятий и рекомендуемой литературе	6
6		Подготовка к контрольной работе №1	2
7	Раздел 6. Метод защиты информации на основе кодового зашумления.	Изучение предусмотренных программой дидактических единиц по конспектам лекций и рекомендуемой литературе	2
8		Выполнение индивидуального домашнего задания и подготовка к защите работы	4
9	Раздел 7. Защита информации на основе временных и спектральных преобразований сигналов.	Изучение предусмотренных программой дидактических единиц по конспектам лекций, материалам практических занятий и рекомендуемой литературе	6
10		Подготовка к контрольной работе №2	2
11	Раздел 8. Защита информации путем разграничения доступа.	Изучение предусмотренных программой дидактических единиц по конспектам лекций и рекомендуемой литературе	2
12	Раздел 9. Защита информации в персональных компьютерах и вычислительных сетях.	Изучение предусмотренных программой дидактических единиц по конспектам лекций, материалам практических занятий и рекомендуемой литературе	6
13		Выполнение индивидуального домашнего задания и подготовка к защите работы	4
14		Подготовка к зачету	6
Всего за 8 семестр			56

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	НЕДЕЛИ СЕМЕСТРА												
	1	2	3	4	5	6	7	8	9	10	11	12	13
8		Тест	ИПЗ		Тест	ДР		ИПЗ	ДЗ	ДР	Тест		диф. зач.

Условные обозначения:

- ДР – диагностическая работа;
- Тест – тест;
- ИПЗ – индивидуальное практическое задание;
- Контр.Р. – контрольная работа;

- ДЗ – домашнее задание;
- диф. зач. – дифференцированный зачет.

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

- диагностическая работа;
- тест;
- индивидуальное практическое задание;
- контрольная работа;
- домашнее задание.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации. М.: КноРус, 2018, 70 экз.
2. И. О. Косых, Л. Б. Кочин. . Методы защиты информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2017, эл. рес.
3. Л. Б. Кочин. . Средства радиоэлектронной защиты. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008, эл. рес.
4. Л. Б. Кочин. . Радиоэлектронная защита: теория и практика. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007, эл. рес.
5. С. А. Нестеров. . Основы информационной безопасности. Санкт-Петербург: Лань, 2022, эл. рес.
6. Ю. И. Коваленко. . Защита информационных технологий. М.: РУСАЙНС, 2016, 30 экз.

5.2. Дополнительная литература по дисциплине:

1. Л. Дж. Хоффман. . Современные методы защиты информации. М.: Сов. радио, 1980, 1 экз.

5.3. Периодические издания:

не требуются.

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

1. <http://e.lanbook.com/> — ЭБС Лань;
2. <http://www.scienceresearch.com/> — Federated Search;
3. <https://urait.ru/> — Главная – Образовательная платформа Юрайт. Для вузов и ссузов.;
4. <http://library.voenmeh.ru/jirbis2/> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

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. Mathcad Education - University Edition Term;
2. Matlab 2015a SP1.

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. Mathcad Education - University Edition Term;
2. Matlab 2015a SP1.

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 **МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ** является дисциплиной **части, формируемой участниками образовательных отношений блока 1**, программы подготовки по направлению *12.03.03 Фотоника и оптоинформатика*. Дисциплина реализуется на факультете И Информационных и управляющих систем БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой И1 ЛАЗЕРНАЯ ТЕХНИКА.

Дисциплина нацелена на формирование *компетенций*:

ПСК-2.1 способность к анализу поставленной задачи исследований в области фотоники и оптоинформатики.

Содержание дисциплины охватывает круг вопросов, связанных с физическими принципами, используемыми для получения, передачи, хранения, обработки информации, компонентами и устройствами систем защиты информации.

Программой дисциплины предусмотрены следующие **виды контроля**:

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

- диагностическая работа;
- тест;
- индивидуальное практическое задание;
- контрольная работа;
- домашнее задание.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

Общая трудоемкость освоения дисциплины составляет **3 з.е., 108 ч**. Программой дисциплины предусмотрены лекционные занятия (**26 ч.**), практические занятия (**26 ч.**), самостоятельная работа студента (**56 ч.**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 52 ч. аудиторных занятий, и 56 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. Понятия и определения дисциплины.		
Изучение предусмотренных программой дидактических единиц по конспектам лекций и рекомендуемой литературе	Л. Б. Кочин. . Средства радиоэлектронной защиты: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008 (введение) Л. Б. Кочин. . Радиоэлектронная защита: теория и практика: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007 (введение)	2
Итого по разделу 1		2
Раздел 2. Общие сведения о криптографической защите информации.		
Изучение предусмотренных программой дидактических единиц по конспектам лекций и рекомендуемой литературе	Л. Б. Кочин. . Радиоэлектронная защита: теория и практика: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007 (1)	2
Итого по разделу 2		2
Раздел 3. Симметричные криптографические системы.		
Изучение предусмотренных программой дидактических единиц по конспектам лекций, материалам практических занятий и рекомендуемой литературе	Л. Б. Кочин. . Средства радиоэлектронной защиты: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008 (1) Л. Б. Кочин. . Радиоэлектронная защита: теория и практика: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007 (1.1.1, 1.1.2)	6
Итого по разделу 3		6
Раздел 4. Несимметричные криптографические системы.		
Изучение предусмотренных программой дидактических единиц по конспектам лекций, материалам практических занятий и рекомендуемой литературе	Л. Б. Кочин. . Средства радиоэлектронной защиты: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008 (1) Л. Б. Кочин. . Радиоэлектронная защита: теория и практика: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007 (1.1.3)	6
Итого по разделу 4		6
Раздел 5. Основы криптографического анализа.		
Изучение предусмотренных программой дидактических единиц по конспектам лекций,	Л. Б. Кочин. . Радиоэлектронная защита: теория и практика: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007	6

материалам практических занятий и рекомендуемой литературе	(1.1, 1.1.4) Л. Б. Кочин. . Средства радиоэлектронной защиты: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008 (1, 2)	
Подготовка к контрольной работе №1		2
Итого по разделу 5		8
Раздел 6. Метод защиты информации на основе кодового зашумления.		
Изучение предусмотренных программой дидактических единиц по конспектам лекций и рекомендуемой литературе	Л. Б. Кочин. . Радиоэлектронная защита: теория и практика: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007 (1.1 -1.3)	2
Выполнение индивидуального домашнего задания и подготовка к защите работы	Л. Б. Кочин. . Средства радиоэлектронной защиты: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008 (1, 2)	4
Итого по разделу 6		6
Раздел 7. Защита информации на основе временных и спектральных преобразований сигналов.		
Изучение предусмотренных программой дидактических единиц по конспектам лекций, материалам практических занятий и рекомендуемой литературе	Л. Б. Кочин. . Радиоэлектронная защита: теория и практика: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007 (1.2 -1.3)	6
Подготовка к контрольной работе №2	Л. Б. Кочин. . Средства радиоэлектронной защиты: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008 (2)	2
Итого по разделу 7		8
Раздел 8. Защита информации путем разграничения доступа.		
Изучение предусмотренных программой дидактических единиц по конспектам лекций и рекомендуемой литературе	Л. Б. Кочин. . Радиоэлектронная защита: теория и практика: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007 (1.4) Л. Б. Кочин. . Средства радиоэлектронной защиты: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008 (4)	2
Итого по разделу 8		2
Раздел 9. Защита информации в персональных компьютерах и вычислительных сетях.		
Изучение предусмотренных программой дидактических единиц по конспектам лекций, материалам практических занятий и рекомендуемой литературе	Ю. И. Коваленко. . Защита информационных технологий: М.: РУСАЙНС, 2016 (все) Л. Б. Кочин. . Радиоэлектронная защита: теория и практика: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007 (1.4, 1.8) Л. Б. Кочин. . Средства радиоэлектронной защиты: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008 (4, 6) С. А. Нестеров. . Основы информационной безопасности: Санкт-Петербург: Лань, 2022 (все)	6
Выполнение индивидуального домашнего задания и подготовка к защите работы	А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (все) Л. Дж. Хоффман. . Современные методы защиты информации: М.: Сов. радио, 1980 (все)	4
Подготовка к зачету	И. О. Косых, Л. Б. Кочин. . Методы защиты информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2017 (все)	6

Итого по разделу 9	16
--------------------	----

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

- диагностическая работа
- тест;
- индивидуальное практическое задание;
- домашнее задание;
- контрольная работа;
- 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.

Тест

Контроль усвоения лекционного материала студентов производится в автоматическом режиме за счет применения ПО «Ментор», представляющего собой веб-приложение, в котором клиентом выступает браузер, а сервером – веб-сервер. Доступ студентов к ПО «Ментор» осуществляется через любой интернет браузер, установленный на любом устройстве, имеющем доступ в сеть Интернет с помощью индивидуального логина и пароля. В конце каждой лекции присутствующим студентам предлагается ответить на один из вопросов по теме изложенной лекции. Результаты тестирования обобщаются с помощью балльно-рейтинговой системы (БАРС). Основным критерием назначения баллов служит способность студента отвечать на тест за минимальное число попыток.

Индивидуальное практическое задание

Решения заданий на практических занятиях представляются в печатной или рукописной форме. Каждое задание содержит три задачи.

Критерии оценивания:

- правильное решение менее 2 задач – 3 баллов,
- каждая правильно решенная задача при общем количестве решенных задач более 2 оценивается в 0,5 балл.

Основанием для снижения количества баллов за одну задачу в диапазоне от 0,5 до 0,2 является небрежное выполнение.

Домашнее задание

Решения домашних заданий представляются в печатной или рукописной форме. Каждое домашнее задание содержит пять задач.

Критерии оценивания:

- правильное решение менее двух задач – 3 балла,
- каждая правильно решенная задача при общем количестве решенных задач более двух оценивается в 0,5 балл.

Основанием для снижения количества баллов за одну задачу в диапазоне от 0,5 до 0,2 является небрежное выполнение.

Контрольная работа

Контрольная работа выполняется в виде письменного решения задачи по пройденным разделам дисциплины. Успешным считается выполнение работы, если студент в основном правильно определил ход решения задачи, выбрал нужные соотношения и получил ответ

Дифференцированный зачет

Итоговый контроль по дисциплине проходит в форме дифференцированного зачета. Зачет по дисциплине оформляется при следующих условиях:

- успешное выполнение всех домашних заданий;
- успешная работа на практических занятиях;

- успешное выполнение заданий контрольных работ.

Зачет включает в себя ответ на теоретические вопросы.

Оценка «зачтено-отлично» выставляется при развернутых и точных ответах на 2 теоретических вопроса.

Оценка «зачтено-хорошо» выставляется при точном и полном ответе на 1-ый теоретический вопрос, и неточном ответе на 2-ой теоретический вопрос.

Оценка «зачтено-удовлетворительно» выставляется либо при правильном ответе на один теоретический вопрос.

Оценка «не зачтено» выставляется при неправильных ответах на теоретические вопросы.

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		ПСК-2.1	
4	8	Раздел 1. Понятия и определения дисциплины.	4	2	2	0	2	10	Тест
4	8	Раздел 2. Общие сведения о криптографической защите информации.	6	4	4	0	2	10	Тест
4	8	Раздел 3. Симметричные криптографические системы.	14	8	4	4	6	12	Тест, Индивидуальное практическое задание
4	8	Раздел 4. Несимметричные криптографические системы.	12	6	2	4	6	12	Тест, Индивидуальное практическое задание
4	8	Раздел 5. Основы криптографического анализа.	18	10	2	8	8	10	Тест, Контрольная работа, Домашнее задание, Индивидуальное практическое задание
4	8	Раздел 6. Метод защиты информации на основе кодового зашумления.	8	2	2	0	6	12	Тест
4	8	Раздел 7. Защита информации на основе временных и спектральных преобразований сигналов.	18	10	4	6	8	12	Тест, Контрольная работа, Индивидуальное практическое задание
4	8	Раздел 8. Защита информации путем разграничения доступа.	4	2	2	0	2	10	Тест
4	8	Раздел 9. Защита информации в персональных компьютерах и вычислительных сетях.	24	8	4	4	16	12	Тест, Домашнее задание
Всего за 8 семестр			108	52	26	26	56	100	
Всего по дисциплине			108	52	26	26	56	100	

Критерии оценивания

ПСК-2.1

Вопросы открытого типа:

- № 1 Перечислите основные принципы обеспечения безопасности
- № 2 Необходимо расшифровать криптограмму, полученную с помощью шифра Цезаря со значением ключа шифрования $K=15$ и криптограмму "съосэъ".
- № 3 Зашифруйте сообщение «БОЛЬШАЯ ПЕРЕМЕНА», используя систему Цезаря со значением ключа $K = 5$.
- № 4 Зашифровать слово «АЛФАВИТ» с помощью шифра Виженера с ключевым словом «СЫР»
- № 5 Что такое атака (attack) по ГОСТ Р ИСО/МЭК 27000-2012?
- № 6 Если длина последовательности $N=256$, то выигрыш от применения алгоритма БПФ составит ____ раз? (берется отношение количества вычисляемых пар операций)
- № 7 Криптографическая защита информации (по ГОСТ Р 50922-2006)- это
- № 8 Что такое коммерческая тайна?
- № 9 Шифрование - это
- № 10 Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию:

Вопросы закрытого типа:

- № 1 Какое определение имеет «информация» для инженеров?
 - Совокупность сведений, подлежащих хранению, передаче, обработке и использованию в человеческой деятельности
 - Совокупность сведений, подлежащих обработке и использованию в человеческой деятельности
 - Сведения (сообщение, данные) независимо от формы их представления
 - Специфический и обязательный атрибут реального мира, представляющий собой его объективное отражение в виде совокупности сигналов и проявляющийся при взаимодействии с «приемником» информации, позволяющие выделять, регистрировать эти сигналы из окружающего мира и по тому или иному критерию их идентифицировать
- № 2 Назовите главное преимущество цифровых каналов связи:
 - простота
 - заданная точность
 - низкая стоимость
 - высокая надежность
- № 3 Что не относится к конфиденциальной информации?
 - Персональные данные
 - Коммерческая тайна
 - Особо важная информация
 - Сведения, содержащиеся в личных делах осужденных, о принудительном исполнении судебных актов
- № 4 Распространение информации подразумевает действия, направленные на получение или передачу информации:
 - определенному кругу лиц
 - неопределённому кругу лиц

- третьим лицам без согласия ее обладателя
 - доступ к которой осуществляется с использованием средств вычислительной техники
- № 5 Что не может составлять коммерческую тайну?
- секрет производства
 - сведения о результатах интеллектуальной деятельности в научно-технической сфере
 - сведения о способах осуществления профессиональной деятельности
 - сведения о численности, о составе работников и о наличии свободных рабочих мест
- № 6 Какие существуют методы обеспечения информационной безопасности?
- Правовые, организационные, экономические
 - Правовые, организационно-технические, экономические
 - Правовые, технические, организационные
 - Правовые, организационно-технологические, экономические
- № 7 Какой метод защиты информации предприятия подразумевает защиту каналов связи, контроль помещений и защиту информации от прослушивания и видеонаблюдения?
- Программно-аппаратный
 - Организационный
 - Технический
 - Правовой
- № 8 Какой метод защиты информации предприятия подразумевает подбор и проверку персонала, мониторинг лояльности персонала и организацию охраны помещений?
- Программно-аппаратный
 - Организационный
 - Технический
 - Правовой
- № 9 Какие виды информации ограниченного доступа существуют?
- Государственная тайна и конфиденциальная информация
 - Служебная тайна и конфиденциальная информация
 - Персональные данные и конфиденциальная информация
 - Государственная тайна и секретная информация
- № 10 Степень схожести одного сигнала на другой дает характеризует:
- переходная характеристика
 - импульсная характеристика
 - корреляционная функция
 - функция Гильберта