МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Саровский физико-технический институт -
филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»
(**СарФТИ НИЯУ МИФИ**)

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЭЛЕКТРОНИКИ

Кафедра «Вычислительной и информационной техники»

УТВЕРЖДАЮ

Декан ФИТЭ, к.ф-м.н.,доцент

_____В.С.Холушкин

«___» _____ 2022 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

наименование дисциплины

Направление подготовки (специальность)	09.03.02 Информационные системы и технологии
Наименование образовательной программы	Информационные системы и технологии в науке и приборостроении
Квалификация (степень) выпускника	бакалавр
Форма обучения	очная

Программа одобрена на заседании кафедры

Протокол_№___от _____

Зав. кафедрой ВИТ

_____ В.С. Холушкин

«____» _____ 2022г.

г. Саров, 2022г.

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ, ФИТЭ на 202____/202_____ учебный год.

Заведующий кафедрой ВИТ В.С. Холушкин

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ, ФИТЭ на 202____/202_____ учебный год.

Заведующий кафедрой ВИТ В.С. Холушкин

Программа переутверждена на 202____/202___учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ, ФИТЭ на 202____/202_____ учебный год.

Заведующий кафедрой ВИТ В.С. Холушкин

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с Семестровыми учебными планами академических групп ФТФ, ФИТЭ на 202____/202_____ учебный год.

Заведующий кафедрой ВИТ В.С. Холушкин

Семестр	В форме практической подготовки	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	КР/ КП	Форма(ы) контроля, экз./зач./ЗсО/	Интерактивные часы
7	32	5	180	16	-	32	96	-	Э	6
ИТОГО	**32**	**5**	**180**	**16**	**-**	**32**	**96**	-	**36**	**6**

АННОТАЦИЯ

Курс посвящен изучению теоретических и практических основ технических средств защиты информации. Изучаются способы и методы разработки современных инструментальных и программных средств защиты информации и их применение при решении научно-исследовательских и производственных задач из различных предметных областей.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина "Технические средства защиты информации" имеет целью обучить студентов основам построения средств и систем защиты информации, применяемым в современной технике, в частности в автоматизированных системах управления, а также облегчить самостоятельную работу студентов с тематической литературой. Дисциплина "Технические средства защиты информации" является продолжением изучения основ вычислительной техники, операционных систем, методов программирования и теории информации.

Задачи дисциплины дать основы:

- системного подхода и теоретического аппарата к проблеме защиты информации;
- построения современных криптографических алгоритмов и протоколов;
- программно-аппаратных реализаций механизмов защиты информации и возможностей по их преодолению.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Технические средства защиты информации» является дисциплиной по выбору общепрофессиональной части и базируется на таких дисциплинах как, «Информатика», «Информационные технологии», «Основы алгоритмизации и программирования», «Технологии программирования», «Архитектура информационных систем». Освоение дисциплины «Технические средства защиты информации» необходимо для последующего применения полученных знаний в профессиональной деятельности.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Процесс изучения дисциплины направлен на формирование следующих компетенций ОС ВО:

Общепрофессиональные компетенции (ОПК)

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
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.	**З-ОПК-2** Знать: принципы функционирования и применения современных информационных технологий **У-ОПК-2** Уметь: применять информационные технологии для решения профессиональных задач. **В-ОПК-2** Владеть: навыками использования современных информационных технологий и программными средствами, в том числе отечественного производства, применять их для решения задач профессиональной деятельности
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**З-ОПК-3** Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **У-ОПК-3** Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **В-ОПК-3** Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
ОПК-4 Способен участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и пра-	**З-ОПК-4** Знать: стандарты, нормы и правила разработки технической документации **У-ОПК-4** Уметь: разрабатывать структуры типовых документов; разрабатывать и оформлять техническую документацию

вил	**В-ОПК-4** Владеть: инструментами и методами разработки Технической документации в профессиональной деятельности

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ*

№ п/п	Наименование раздела /темы дисциплины	№ недели	Виды учебной работы					
			Лекции	Практ. занятия/ семинары	Лаб. работы	СРС	Текущий контроль (форма)*	Максимальный балл (см. п. 5.3)
			16	-	32	96		
Семестр 7								
Раздел 1.								
1.1.	Тема1. Основные понятия о защите информации	**1,2**	**2**		**4**	**16**	**УО**	**4**
Раздел 2.								
2.1	Тема 1.Возможные каналы утечки информации	**3,4**	**2**		**4**	**16**	**Защита ЛР**	**4**
2.2	Тема 2.Методы противодействия утечке информации по возможным каналам утечки информации	**5,6**	**2**		**4**	**16**	**УО**	**4**
2.3	Тема 3. Нормативные документы, регламентирующие порядок защиты информации в технических системах	**7,8**	**2**		**4**	**16**	**Защита ЛР**	**4**
2.4	Тема 4.Методы расчета и инструментального контроля показателей защиты информации	**9,10**	**2**		**8**	**16**	**Защита ЛР**	**4**

№ п/п	Наименование раздела /темы дисциплины	№ недели	Виды учебной работы					
			Лекции	Практ. занятия/ семинары	Лаб. работы	СРС	Текущий контроль (форма)*	Максимальный балл (см. п. 5.3)
			16	-	32	96		
	Рубежный контроль	**11**					**СР**	**7**
Раздел 3.								
3.1	Тема 1. Программно-аппаратная реализация средств обеспечения информационной безопасности	**12-15**	**6**		**8**	**16**	**Защита ЛР**	**8**
	Рубежный контроль	**16**					**СР**	**10**
	Промежуточная аттестация					**Э**	**-**	**50**
	Посещаемость							**5**
	Итого:		**16**		**32**	**96**	**-**	**100**

***Сокращение наименований форм текущего, рубежного и промежуточного контроля:**

УО – устный опрос

СР – самостоятельная работа(решение задачи на заданную тему)

РГР – расчетно – графическая работа

4.2. Содержание дисциплины, структурированное по разделам (темам)

Лекционный курс

№	Наименование раздела /темы дисциплины	Содержание
	7 семестр	
	Раздел 1.	
1.1	Тема 1. Основные понятия о защите информации	Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения и сигналов. Опасные сигналы и их источники. Побочные электромагнитные излучения и наводки.
	Раздел 2.	
2.1	Тема 1.Возможные каналы утечки информации	Структура, классификация и основные характеристики технических каналов утечки информации. Классификация технической разведки. Основные этапы и

		процедуры добывания информации технической разведкой. Возможности видов технической разведки.
2.2	Тема 2.Методы противодействия утечке информации по возможным каналам утечки информации	Концепция и методы инженерно-технической защиты информации. Методы и средства инженерной защиты и технической охраны объектов. Скрытие объектов наблюдения. Скрытие речевой информации в каналах связи. Энергетическое скрытие акустических информативных сигналов. Обнаружение и локализация закладных устройств, подавление их сигналов. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания. Подавление опасных сигналов
2.3	Тема 3. Нормативные документы,регламентирующие порядок защиты информации в технических системах	Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке.
2.4	Тема 4.Методы расчета и инструментального контроля показателей защиты информации	Виды контроля эффективности защиты информации. Основные положения методологии инженерно-технической защиты информации. Методы расчета и инструментального контроля показателей защиты информации
Раздел 3.		
3.1	Тема 1. Программно-аппаратная реализация средств обеспечения информационной безопасности	Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности. Программно-аппаратные средства защиты информации в сетях передачи данных.

Лабораторные занятия

№ п/п	Наименование лабораторной работы
1	Генератор паролей с заданными требованиями
2	Генератор паролей и оценка стойкости полученных паролей по отношению к атакам методом прямого перебора
3	Шифрование входного потока информации по заданному алгоритму с обязательным дешифрованием
4	Стеганография: метод незначащих младших разрядов (Least Significant Bit). Использование контейнеров формата Bitmap

4.3. Перечень учебно-методического обеспечения для самостоятельной работы студентов

При изучении дисциплины используются следующие виды самостоятельной работы:

- самостоятельный поиск литературы по разделам и темам курса;
- изучение материала по дополнительным разделам дисциплины;
- изучение литературы и подготовка к выполнению лабораторных работ;
- подготовка к тестированию, контрольным работам, написанию рефератов;
- подготовка к экзамену.

  Форма контроля: отчет по лабораторным работам и их защита.

Рекомендуемый перечень тем для самостоятельного изучения:

- Модель системы защиты. Варианты усиления систем защиты. Характеристика прочности контролируемой преграды. Модель системы защиты. Характеристика прочности неконтролируемой преграды.
- Каналы несанкционированного доступа. Штатные каналы доступа к информации. Возможные каналы несанкционированного доступа к информации. Отличия штатных и нештатных каналов/
- Системы охранной сигнализации. Наружные системы охраны.
- Системы контроля вскрытия аппаратуры (СКВА). Особенности применения СКВА. Требования к СКВА. Принципы построения СКВА.
- Системы контроля и разграничения доступа к информации. Признаки деления информации на группы доступа. Методы разграничения полномочий пользователей. Системы биометри-

ческой идентификации.

- Носители кодовой информации. Основные требования к носителям. Примеры основных типов носителей.
- Контроль целостности программного обеспечения и информации. Применяемые методы. Сравнительная оценка методов контрольной суммы и хэш-функции. Контроль с использованием циклических кодов. Методы дублирования
- Средства защиты программного обеспечения от несанкционированной загрузки. Предпринимаемые меры обеспечения безопасности.
- Защита информации в линиях связи. Средства обеспечения безопасности.
- Средства регистрации доступа к информации. Регистрируемые события. Способы регистрации.
- Организационные мероприятия по защите информации в автоматизированной системе.
- Межсетевые экраны. Схема построения. Основные функции/

1.А.П.Мартынов, В.Н.Фомченко. Криптография и электроника. / Под ред. А.И. Астайкина. Саров:ФГУП «РФЯЦ-ВНИИЭФ», 2006.

2.Н.Я.Виленкин. Комбинаторика. М., Наука,1969.

3.В.Фелер. Введение в теорию вероятностей и ее применение и ее применение. Пер. с англ. т.1, М., Мир, 1984; т.2, М., Мир, 1984.

4.А.Г.Конхейм. Основы криптографии. Пер. с англ. под ред. В.А.Герасименко. М., Радио и связь, 1987.

5.К.Е.Шеннон. Теория связи секретных систем. 1949.

6.Дж.Л.Месси Введение в современную криптологию. ТИИЭР, т.76, №5, 1988.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

5.1. Паспорт фонда оценочных средств по дисциплине

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Раздел	Темы занятий	Компетенция	Индикаторы освоения	Текущий контроль, неделя
Семестр 7				
Раздел 1	Тема 1.Возможные каналы утечки информации	ОПК-2,ОПК-3,ОПК-4	З-ОПК-2; У-ОПК-2; В-ОПК-2 З-ОПК-3; У-ОПК-3; В-ОПК-3 З-ОПК-4; У-ОПК-4; В-ОПК-4	УО2
Раздел 2	Тема 2.Методы противодействия утечке информации по возможным каналам утечки информации	ОПК-2,ОПК-3,ОПК-4	З-ОПК-2; У-ОПК-2; В-ОПК-2 З-ОПК-3; У-ОПК-3; В-ОПК-3 З-ОПК-4; У-ОПК-4; В-ОПК-4	Защита ЛР 4
	Тема 3. Нормативные документы, регламентирующие порядок защиты информации в технических системах		З-ОПК-2; У-ОПК-2; В-ОПК-2 З-ОПК-3; У-ОПК-3; В-ОПК-3 З-ОПК-4; У-ОПК-4; В-ОПК-4	УО6 Защита ЛР6
	Тема 4.Методы расчета и инструментального контроля показателей защиты информации		З-ОПК-2; У-ОПК-2; В-ОПК-2 З-ОПК-3; У-ОПК-3; В-ОПК-3 З-ОПК-4; У-ОПК-4; В-ОПК-4	Защита ЛР 8
	Тема 1.Возможные каналы утечки информации		З-ОПК-2; У-ОПК-2; В-ОПК-2 З-ОПК-3; У-ОПК-3; В-ОПК-3 З-ОПК-4; У-ОПК-4; В-ОПК-4	Защита ЛР 10
Рубежный контроль		ОПК-2,ОПК-3,ОПК-4	З-ОПК-2; У-ОПК-2; В-ОПК-2 З-ОПК-3; У-ОПК-3; В-ОПК-3 З-ОПК-4; У-ОПК-4; В-ОПК-4	СР 8
Раздел 3	Тема 1. Программно-аппаратная реализация средств обеспечения информационной безопасности	ОПК-2,ОПК-3,ОПК-4	З-ОПК-2; У-ОПК-2; В-ОПК-2 З-ОПК-3; У-ОПК-3; В-ОПК-3 З-ОПК-4; У-ОПК-4; В-ОПК-4	Защита ЛР 10
Рубежный контроль		ОПК-2,ОПК-3,ОПК-4	З-ОПК-2; У-ОПК-2; В-ОПК-2 З-ОПК-3; У-ОПК-3; В-ОПК-3 З-ОПК-4; У-ОПК-4; В-ОПК-4	СР 16
Промежуточная аттестация		ОПК-2,ОПК-3,ОПК-4	З-ОПК-2; У-ОПК-2; В-ОПК-2 З-ОПК-3; У-ОПК-3; В-ОПК-3 З-ОПК-4; У-ОПК-4; В-ОПК-4	**Экзамен**

5.2.1. Оценочные средства для текущего контроля

5.2.1.1. Примерные вопросы для устного опроса (УО)

1. Основные понятия о защите информации.
2. Виды, источники и носители защищаемой информации.
3. Демаскирующие признаки объектов наблюдения и сигналов.
4. Опасные сигналы и их источники.
5. Побочные электромагнитные излучения и наводки.
6. Возможные каналы утечки информации.
7. Структура, классификация и основные характеристики технических каналов утечки информации.

8. Классификация технической разведки.
9. Основные этапы и процедуры добывания информации технической разведкой.
10. Возможности видов технической разведки.

5.2.2. Оценочные средства для рубежного контроля

5.2.2.1 Примерные задания для решения задач по заданной теме

1. Произвести преобразование информации с использованием изученных простейших шифров.

2. Произвести преобразование информации с использованием основных криптографических операций и их композиций.

3. Вычислить статистические характеристики предложенных информационных блоков и восстановить данные с использованием элементов статистического анализа.

4. Получить последовательности с заданными свойствами, используя методы и алгоритмы формирования псевдослучайных последовательностей информации.

5. Осуществить преобразование информации с использованием функций криптоалгоритма «Люцифер».

6. Осуществить преобразование информации с использованием функций криптоалгоритма DES.

7. Осуществить преобразование информации с использованием функций криптоалгоритма ГОСТ 28147-89.

8. Осуществить преобразование информации с использованием функций одного из изученных блочных симметричных криптоалгоритмов.

9. Осуществить преобразование информации с использованием функций одного из изученных криптоалгоритмов с открытым ключом

10. Осуществить формирование хэш-значения и последующее получение электронной цифровой подписи с использованием соответствующих алгоритмов изученных в процесс преподавания дисциплины.

5.2.3. Оценочные средства для промежуточной аттестации

5.2.3.2. Примерные вопросы к экзамену

1. Основные понятия о защите информации.
2. Виды, источники и носители защищаемой информации.
3. Демаскирующие признаки объектов наблюдения и сигналов.
4. Опасные сигналы и их источники.
5. Побочные электромагнитные излучения и наводки.
6. Возможные каналы утечки информации.
7. Структура, классификация и основные характеристики технических каналов утечки информации.
8. Классификация технической разведки.
9. Основные этапы и процедуры добывания информации технической разведкой.
10. Возможности видов технической разведки.
11. Методы противодействия утечке информации по возможным каналам утечки информации.
12. Концепция и методы инженерно-технической защиты информации.
13. Методы и средства инженерной защиты и технической охраны объектов.
14. Скрытие объектов наблюдения.
15. Скрытие речевой информации в каналах связи.
16. Энергетическое скрытие акустических информативных сигналов.
17. Обнаружение и локализация закладных устройств, подавление их сигналов.
18. Подавление опасных сигналов акустоэлектрических преобразователей.
19. Экранирование и компенсация информативных полей.
20. Подавление информативных сигналов в цепях заземления и электропитания.
21. Подавление опасных сигналов.
22. Нормативные документы, регламентирующие порядок защиты информации в технических системах.
23. Характеристика государственной системы противодействия технической разведке
24. Нормативные документы по противодействию технической разведке.
25. Методы расчета и инструментального контроля показателей защиты информации.
26. Виды контроля эффективности защиты информации.
27. Основные положения методологии инженерно-технической защиты информации.
28. Методы расчета и инструментального контроля показателей защиты информации

28. Программно-аппаратная реализация средств обеспечения информационной безопасности.
29. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
30. Программно-аппаратные средства защиты информации в сетях передачи данных.

5.3. Шкалы оценки образовательных достижений

Рейтинговая оценка знаний является интегральным показателем качества теоретических и практических знаний и навыков студентов по дисциплине и складывается из оценок, полученных в ходе текущего контроля и промежуточной аттестации.

Результаты текущего контроля и промежуточной аттестации подводятся по шкале балльно-рейтинговой системы.

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td><td rowspan="2">Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.</td></tr>
<tr><td>60-64</td><td>E</td></tr>
</table>

Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Рекомендуемая литература

ОСНОВНАЯ:

1.А.П.Мартынов, В.Н.Фомченко. Криптография и электроника. / Под ред. А.И. Астайкина. Саров:ФГУП «РФЯЦ-ВНИИЭФ», 2006.

2.Н.Я.Виленкин. Комбинаторика. М., Наука,1969.

3.В.Фелер. Введение в теорию вероятностей и ее применение и ее применение. Пер. с англ. т.1, М., Мир, 1984; т.2, М., Мир, 1984.

4.А.Г.Конхейм. Основы криптографии. Пер. с англ. под ред. В.А.Герасименко. М., Радио и связь, 1987.

5.К.Е.Шеннон. Теория связи секретных систем. 1949.

6.Дж.Л.Месси Введение в современную криптологию. ТИИЭР, т.76, №5, 1988.

7.А.П.Мартынов, Д.Б.Николаев, А.В.Аграновский, А.В.Балакин, Р.А.Хади, В.Н.Фомченко. Разработка архитектуры программного комплекса информационной защиты ведомственной локальной сети и рабочих станций. Учебно-методическое пособие. - Саров: «ИНФО», 2003.

8.А.П.Мартынов, Д.Б.Николаев, Н.П.Волошин, В.Н.Фомченко. Алгоритмы криптографического преобразования. Симметрические и асимметрические криптографические системы, и криптографические протоколы. Учебно-методическое пособие. - Саров: «ИНФО», 2002. пособие. - Саров: «ИНФО», 2002. - 65 с: ил.

9.А.А.Курочкин, А.П.Мартынов. Статистический и вероятностный анализ источников сообщения криптографических систем. Учебно-методическое пособие. - Саров: «ИНФО», 2002.

10.А.А.Курочкин, А.П.Мартынов, С.В.Панкратов, В.Н.Фомченко. Теоретическая стойкость криптографических систем. Учебно-методическое пособие.

ДОПОЛНИТЕЛЬНАЯ:

1.А.Ахо. Дж.Хопкрофт, Дж.Ульман. Построение и анализ вычислительных алгоритмов. Пер. с англ., М. Мир, 1975.

2.Х.Файстелл, У.Хотц, Дж.Смит. Криптографические методы в межмашинном обмене информацией. ТИИЭР, 1975,т.63, №11.

3.А.П.Мартынов, Д.Б.Николаев, В.Н.Фомченко, С.А.Сапожников, В.Г.Грибунин. Введение в стеганографию. Учебно-методическое пособие. -Серпухов: Типография СВИРВ. 2004.

4.Г.Крамер. Математические методы статистики. Пер. с англ., М., Мир, 1975.

5.А.П.Мартынов, Д.Б.Николаев, А.В.Аграновский, С.Н.Гончаров, Д.А.Леднов, С.А.Репалов, В.Н.Фомченко. Исследование построения систем идентификации по речевым характеристикам - Саров: «ИНФО», 2003.

6.АА.Грушо, Е.Е.Тимонина. Теоретические основы защиты информации. М.: Издательство агентства "Яхтсмен", - 1996.

7.Солтцер, Шредер. Защита информации в вычислительных системах. ТИИЭР, т.63, №9, сентябрь 1975.

8.Толковый словарь по вычислительным системам. М., Машиностроение, 1990.

9.Дж.Л.Месси. Введение в современную криптологию. ТИИЭР, т.76, №5, май 1988.

10.А.А.Курочкин, А.П.Мартынов. Методы синтеза цифровых преобразующих устройств каналов связи, Учебно-методическое пособие.- Саров: «ИНФО», 2002.

11.А.А.Курочкин, А.П.Мартынов. Способы кодирования цифровой информации для ее передачи по последовательным каналам связи. Учебно-методическое пособие. - Саров: «ИНФО», 2003.

12.А.П.Мартынов, Д.Б.Николаев. Электронные кодовые переключатели. Учебно-методическое пособие. - Саров: «ИНФО», 2002.

УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ:

1.Д.Б.Николаев. Технические средства защиты информации. Конспект лекций.

2. А.П.Мартынов, Д.Б.Николаев. Основы криптографии. Конспект лекций. 3.А.П.Мартынов, Д.Б.Николаев. Криптография и специсследования. Конспект лекций.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Изучение дисциплины проводится в лабораториях кафедры «Вычислительная и информационная техника». Лабораторные работы проводятся с использованием ресурсов компьютерных классов, позволяющих работать в различных инструментальных средах.

Класс ПЭВМ не ниже Intel Pentium 4, 512M RAM, 40G HDD с установленным программным обеспечением: MS WindowsXP, MS Office Pro, Borland Delphi 7.0, Microsoft Visual Studio 6.0, интерпретатор PHP 5.0, интерпретатор PERL 5.0
Из расчета одна ПЭВМ на одного человека.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В соответствии с требованиями ОС ВО по направлению подготовки 09.03.02 «Информационные системы и технологии» реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В рамках учебного курса студенты работают с лекциями, рекомендованной литературой, выполняют лабораторные работы, готовятся к экзамену и зачету. В процессе подготовки студенты используют программные продукты, инструментальные среды, информационно-справочные системы, информационные источники, размещенные в сети Интернет (официальные сайты, веб-порталы, тематические форумы и телекоммуникации), электронные учебники и учебно-методические пособия.

9. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ СТУДЕНТАМ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

- Самостоятельно прорабатывать лекционный материал для более полного усвоения материала;
- В учебном процессе при выполнении лабораторного практикума эффективно использовать методические пособия и методический материал по темам лабораторных работ;
- Активно использовать Интернет-ресурсы для получения актуального материала по изучаемой дисциплине;
- Активно использовать Интернет-ресурсы для обновления инструментальной базы (систем программирования, инструментальных сред и т.д.) при выполнении лабораторных работ.

Программа составлена в соответствии с требованиями ОС ВО НИЯУ МИФИ к обязательному минимуму содержания основной образовательной программы по направлению подготовки 09.03.02 Информационные системы и технологии

Автор(ы) _____М.Д. Романова

Рецензент _____Д.Б. Николаев

Согласовано:

Зав. кафедрой ВИТ _____ В.С. Холушкин

Руководитель ОП _____ В.С. Холушкин