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

ЗАЩИТА 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	10
ИТОГО	**32**	**5**	**180**	**16**	**-**	**32**	**96**	-	**36**	**10**

АННОТАЦИЯ

Курс посвящен изучению теоретических и практических основ 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 УСВОЕНТЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью дисциплины является обучение студентов современным технологиям защиты информации, знакомство с программно-аппаратными средствами в виде электронных ключей, изучение основных приемов построения программных систем защиты информации. Задачей дисциплины является изучение основ защиты информации в современных вычислительных и телекоммуникационных системах, являющихся базовыми для построения, тестирования и технической эксплуатации защищенных информационных систем

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЕ В СТРУКТУРЕ ООП ВО

Дисциплина «Защита информации» является базовой (общепрофессиональной) частью профессиональной компетенции и базируется на таких дисциплинах как, «Информатика», «Информационные технологии», «Алгоритмические языки», «Программирование».

Освоение дисциплины «Защита информации» необходимо для успешного изучения дисциплин, связанных с проектированием и эксплуатацией информационных систем с применением современных методов защиты информации. Знание основ защиты информации в рамках информационных систем необходимо для успешного выполнения производственной практики и научно-исследовательской работы бакалавра.

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: источники информации, необходимой для решения задач профессиональной деятельности; принципы обеспечения безопасности при работе с информационными системами У-ОПК-3 Уметь: осуществлять поиск необходимой информации для решения задач профессиональной деятельности на основе информационной и библиографической культуры В-ОПК-3 Владеть: методами поиска информации в локальных и глобальных сетях с соблюдением требований информационной безопасности
ОПК-4 Способен участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил	**З-ОПК-4** Знать: стандарты, нормы и правила разработки технической документации **У-ОПК-4** Уметь: разрабатывать структуры типовых документов; разрабатывать и оформлять техническую документацию **В-ОПК-4** Владеть: инструментами и методами разработки технической документации в профессиональной деятельности

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ*

№	Наименование раз-	№ не-	Виды учебной работы

п/п	дела /темы дисциплины	дели	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, уровни информационной безопасности, составные части системы защиты информации (СЗИ)	**1**	**1**		**2**	**6**	**УО**	**2**
1.2	Тема 2. Проблемы безопасности программного обеспечения. Угрозы информационным ресурсам	**2**	**1**		**2**	**6**	**УО**	**2**
1.3	Тема 3.Методы и средства защиты информации	**3**	**1**		**2**	**6**	**УО**	**2**
1.4	Тема 4. Идентификация и аутентификация пользователя в системах управления доступом. Модели систем управления доступом	**4**	**2**		**2**	**6**	**УО**	**3**
Раздел 2.								
2.1	Тема 1. Тема 2. СЗИ с принудительным назначением паролей. Виды и надежность паролей	**5**	**2**		**2**	**6**	**Защита ЛР**	**3**
2.2	Тема 2. Биометрические методы идентификации пользователя	**6**	**2**		**2**	**6**	**УО**	**3**
2.3	Тема 3. Компьютерная стеганография	**7**	**1**		**2**	**6**	**Защита ЛР**	**3**

№ 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		
2.4	Тема 4. Криптографические методы и средства защиты информации	8	1		2	6	Защита ЛР	3
Рубежный контроль		9					СР	4
Раздел 3.								
3.1	Тема 1. Государственные стандарты - алгоритмы шифрования DES и RSA	10	1		2	6		3
3.2	Тема 2 Государственные стандарты - алгоритм шифрования ГОСТ-28147-89	11-12	1		2	6		3
3.3	Тема 3.Хэширование: пароли, ключи, ЭЦП	13-14	1		4	12	Защита ЛР	3
3.4	Тема 4. Защита операционных систем. Защита электронного документооборота. Защита от вирусов. Защита от хакеров	15	1		4	12		3
3.5	Тема 5. Правовое обеспечение защиты информации ограниченного доступа	16	1		4	12		3
Рубежный контроль		17					СР	5
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, уровни информационной безопасности, составные части системы защиты информации (СЗИ). .	Важность и сложность проблемы информационной безопасности нарушения; механизмы и службы защиты; модели защиты информации, компьютерных систем и сетей. Организационно-технические и режимные меры. Программно-технические методы и средства защиты информации.
1.2	Тема 2 Проблемы безопасности программного обеспечения. Угрозы информационным ресурсам.	Назначение и состав системы программирования. Классификация языков программирования. Инструментальная среда Microsoft Visual Studio 15. Система программирования Visual C++.
1.3	Тема 3 Методы и средства защиты информации	Программные**,** технические, организационные, административные, правовые. Устройства защиты от утечки информации по каналам ПЭМИН. Методика противодействия несанкционированной аудио- и видеозаписи. Требования и рекомендации Гостехкомиссии по защите информации от утечки по техническим каналам. **Оценка защищенности информации от утечки по каналам ПЭМИН**. Оценочные стандарты и технические спецификации;«Оранжевая книга» как оценочный стандарт; информационная безопасность распределенных систем; рекомендации X.800; стандарт ISO/IEC 15408; «критерии оценки безопасности информационных технологий»; гармонизированные критерии Европейских стран; интерпретация «Оранжевой книги» для сетевых конфигураций;

		руководящие документы Гостехкомиссии России.
1.4	Тема 4. Идентификация и аутентификация пользователя в системах управления доступом.	Задачи аутентификации в компьютерных системах. Строгая аутентификация, непрямая, аппаратные и биометрические средства. Комплексное решение схем строгой аутентификации при предоставлении удаленного доступа к информационным ресурсам.
Раздел 2.		
2.1	Тема 1. СЗИ с принудительным назначением паролей. Виды и надежность паролей.	Применение пароля для подтверждения подлинности пользователя. Клавиатурные, электронные, биометрические, смешанные пароли. Требования надежности. Атаки на парольные системы. Администрирование систем управления пользователями, принудительное назначение и смена паролей
2.2	Тема 2. Биометрические методы идентификации пользователя	Группы биометрических параметров, предъявляемых пользователем. Биометрические системы защиты информации и оценка их качества. Наиболее распространенные и наиболее надежные биометрические системы, сферы их применения.
2.3	Тема 3. Компьютерная стеганография	Обзор традиционных методов стеганографии, их классификация. Компьютерная реализация: использование особенностей файловой системы; использование избыточности, присущей файлам формата multi-media. Метод незначащих младших разрядов – Least Significant Bit.
2.4	Тема 4. Криптографические методы и средства защиты информации.	Исторические этапы становления современной криптографии. Модели криптографии К. Шеннона; теоретико-информационные оценки стойкости симметричных криптосистем с секретным ключом; потоковые шифры; блочные шифры. Абсолютно стойкий шифр. Применение режима однократного гаммирования. Шифрование (кодирование) исходных текстов одним ключом по различным криптоалгоритмам. Несимметричные криптоси-

		стемы с открытым ключом. Схема электронно-цифровой подписи (ЭЦП). Криптографичекие хэш-функции
Раздел 3.		
3.1	Тема 1. Государственные стандарты - алгоритмы шифрования DES и RSA.	Блочные симметричные криптосистемы с секретным ключом. Простота и надежность сетей Фейстеля – основы алгоритма DES. Схема DES на примере одного раунда, расширение и сжатие шифруемых блоков, перестановка при помощи таблиц S-boxes, генерация подключей. Несимметричные системы с открытым ключом – алгоритм RSA, свойства простых чисел, генерация простых чисел, пространство ключей, слабые ключи.
3.2	Тема 2. Государственные стандарты - алгоритм шифрования ГОСТ-28147-89.	Надежность алгоритма, схема преобразования на примере одного раунда. Влияние длины ключа на надежность криптосистем.
3.3	Тема 3. Хэширование	Понятие односторонней или необратимой функции. Требования к хэш-функции. Пример алгебраических хэш-функций. Пример блочного хэша. Современные системы хэширования: семейство MD4/MD5
3.4	Тема 4. Защита операционных систем. Защита электронного документооборота. Защита от вирусов. Защита от хакеров.	Уязвимость операционных систем, метод “заплаток”. Наличие встроенных механизмов безопасности. Проблемы спама, применение фильтров и “черных списков”. История появления и развития вирусов. Вредоносное программное обеспечение, шпионское ПО, последствия заражения. Программные средства защиты от вирусного вторжения. Хакерство и пиратство - традиционные приемы и современные разработки в этой области. Способы и средства защиты. Организационные-административные и правовые меры борьбы с нарушителями информационной безопасности
3.5	Тема 5. Правовое обеспече-	Определение информации, подлежащей защите. Защита

	ние защиты информации ограниченного доступа	государственной тайны. Государственная система и нормативно-правовая база защиты информации в РФ. Функции, состав и перспективы развития государственной системы защиты информации. Законодательство РФ в области защиты информации.

Лабораторные занятия

№ п/п	Примерные темы лабораторных занятий
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

1. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. Учебное пособие.- Издательство: Инфра - М; Серия: Высшее образование; 304 стр., 2001
2. Домарев В.В. Защита информации и безопасность компьютерных систем ДиаСофт, 1999, 480 с.
3. Петров А.А. Компьютерная безопасность. Криптографические методы защиты.- М.:ДМК,2000.-448 с.
4. Курс лекций по защите информации. Романова М.Д. Электронный ресурс СарФТИ НИЯУ МИФИ. 2021

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 1				
Раздел 1	Тема1. Основные понятия, уровни информационной безопасности, составные части системы защиты информации (СЗИ).	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	УО 1
	Тема 2. Проблемы безопасности программного обеспечения. Угрозы информационным ресурсам		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	УО 2
	Тема 3.Методы и средства 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	УО 3
	Тема 4. Идентификация и аутентификация пользователя в системах управления доступом. Модели систем управления доступом		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	УО 4
Раздел 2	Тема 1. СЗИ с принудительным назначением паролей. Виды и надежность паролей	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 5
	Тема 2. Биометрические методы идентификации пользователя		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	УО 6

	Тема3. Компьютерная стеганография		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 7
	Тема 4. Криптографические методы и средства 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
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. Государственные стандарты - алгоритмы шифрования DES и RSA	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	УО 9
	Тема 2 Государственные стандарты - алгоритм шифрования ГОСТ-28147-89		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	УО 10
	Тема 3.Хэширование: пароли, ключи, ЭЦП		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 11-12
	Тема 4. Защита операционных систем. Защита электронного документооборота. Защита от вирусов. Защита от хакеров		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	УО 13-14
	Тема 5. Правовое обеспечение защиты информации ограниченного доступа		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	УО 15
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. Виды паролей и их надежность
2. Атаки на пароли методом прямого перебора
3. Нестандартные пароли
4. Электронные ключи
5. Надежность биометрических идентификаторов
6. Простейшие криптоалгоритмы
7. Комплексные СЗИ
8. Правила и требования безопасности в организации и на предприятии

5.2.2. Оценочные средства для рубежного контроля

5.2.2.1 Примерные задания для решения задач по заданной теме

1. Разработать консольное приложение - генератор паролей с заданными требованиями
2. Разработать визуальное приложение - генератор паролей с заданными требованиями
3. Провести количественную оценку стойкости полученного пароля
4. Разработать приложение, генерирующее пароли и выполняющее оценку их стойкости по отношению к атакам методом прямого перебора
5. Реализовать один из предложенных криптоалгоритмов
6. Реализовать собственный криптоалгоритм
7. Реализовать процедуру перемешивания двоичных блоков, предваряющую процесс шифрования
8. Реализовать процедуру сжатия двоичных шифроблоков по заданным S-таблицам

5.2.3. Оценочные средства для промежуточной аттестации

5.2.3.2. Примерные вопросы к экзамену

1. Основные понятия, уровни информационной безопасности

2. Составные части системы защиты информации (СЗИ).
3. Программно-технические методы и средства защиты информации.
4. Проблемы безопасности программного обеспечения.
5. Угрозы информационным ресурсам.
6. Методы и средства защиты информации.
7. Программные, технические, организационные, административные, правовые.
8. Устройства защиты от утечки информации по каналам ПЭМИН.
9. Методика противодействия несанкционированной аудио- и видеозаписи.
10. Требования и рекомендации Гостехкомиссии по защите информации от утечки по техническим каналам.
11. Оценка защищенности информации от утечки по каналам ПЭМИН.
12. Идентификация и аутентификация пользователя в системах управления доступом.
13. Задачи аутентификации в компьютерных системах.
14. Строгая аутентификация, непрямая, аппаратные и биометрические средства.
15. Комплексное решение схем строгой аутентификации при предоставлении удаленного доступа к информационным ресурсам.
16. СЗИ с принудительным назначением паролей. Виды и надежность паролей.
17. Применение пароля для подтверждения подлинности пользователя.
18. Клавиатурные, электронные, биометрические, смешанные пароли.
19. Требования надежности. Атаки на парольные системы.
20. Администрирование систем управления пользователями, принудительное назначение и смена паролей
21. Биометрические методы идентификации пользователя.
22. Группы биометрических параметров, предъявляемых пользователем.
23. Биометрические системы защиты информации и оценка их качества.
24. Наиболее распространенные и наиболее надежные биометрические системы, сферы их применения.
25. Компьютерная стеганография.
26. Обзор традиционных методов стеганографии, их классификация.
27. Компьютерная реализация: использование особенностей файловой системы; использование избыточности, присущей файлам формата multi-media.
28. Метод незначащих младших разрядов – Least Significant Bit.

29. Криптографические методы и средства защиты информации. Исторические этапы становления современной криптографии.
30. Модели криптографии К. Шеннона; теоретико-информационные оценки стойкости симметричных криптосистем с секретным ключом; потоковые шифры; блочные шифры.
31. Абсолютно стойкий шифр. Применение режима однократного гаммирования.
32. Шифрование (кодирование) исходных текстов одним ключом по различным криптоалгоритмам.
33. Несимметричные криптосистемы с открытым ключом.
34. Схема электронно-цифровой подписи (ЭЦП). Криптографические хэш-функции.
35. Государственные стандарты - алгоритмы шифрования DES и RSA.
36. Блочные симметричные криптосистемы с секретным ключом.
37. Простота и надежность сетей Фейстеля – основы алгоритма DES.
38. Схема DES на примере одного раунда, расширение и сжатие шифруемых блоков, перестановка при помощи таблиц S-boxes, генерация подключей.
39. Несимметричные системы с открытым ключом – алгоритм RSA, свойства простых чисел, генерация простых чисел, пространство ключей, слабые ключи.
40. Государственные стандарты - алгоритм шифрования ГОСТ-28147-89.
41. Надежность алгоритма, схема преобразования на примере одного раунда. Влияние длины ключа на надежность криптосистем.
42. Хэширование.
43. Понятие односторонней или необратимой функции. Требования к хэш-функции.
44. Пример алгебраических хэш-функций. Пример блочного хэша.
45. Современные системы хэширования: семейство MD4/MD5
46. Защита операционных систем.
47. Защита электронного документооборота.
48. Защита от вирусов.
49. Защита от хакеров.
50. Уязвимость операционных систем, метод “заплаток”.
51. Наличие встроенных механизмов безопасности. Проблемы спама, применение фильтров и “черных списков”.
52. История появления и развития вирусов. Вредоносное программное обеспечение, шпионское ПО, последствия заражения.

53. Программные средства защиты от вирусного вторжения.
54. Хакерство и пиратство - традиционные приемы и современные разработки в этой области. Способы и средства защиты.
55. Организационно-административные и правовые меры борьбы с нарушителями информационной безопасности.
56. Правовое обеспечение защиты информации ограниченного доступа.
57. Определение информации, подлежащей защите. Защита государственной тайны.
58. Государственная система и нормативно-правовая база защиты информации в РФ.
59. Функции, состав и перспективы развития государственной системы защиты информации. Законодательство РФ в области защиты информации.

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:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	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.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал,
75-84		C	

70-74		D	грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
65-69	3 – «*удовлетворительно*»		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.
60-64		E	
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

1. Драга А.А. Обеспечение безопасности предпринимательской деятельности: Практическое пособие сотрудников частных служб безопасности, предпринимателей, студентов. – М.: Изд. МГТУ им. Баумана. 1998 – 304с.
2. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. Учебное пособие.- Издательство: Инфра - М; Серия: Высшее образование; 304 стр., 2001
3. Домарев В.В. Защита информации и безопасность компьютерных систем ДиаСофт, 1999, 480 с.
4. Петров А.А. Компьютерная безопасность. Криптографические методы защиты.- М.:ДМК,2000.-448 с.
5. Бабенко Л.К. Методическое пособие. Организация и технология защиты информации. -ТРТИ, Таганрог 1999.-50 с.
6. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. Москва - 2001, 148с/

7. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации. Санкт-Петербург, 1997 – 272с
8. Мельников В. Защита информации в компьютерных системах. Москва 1997 – 368с
9. Барсуков В.С., Водолазкий В.В. Современные технологии безопасности. Москва 2000 – 496с
10. Крысин А. Информационная безопасность. Практическое руководство. Киев 2003 – 320с
11. Советов Б.Я. Информационные технологии: Учебник для вузов. Москва:Высш. шк., 2003 – 263с
12. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы. Электронная версия в формате PDF
13. Винокуров А. Алгоритм шифрования ГОСТ28147-89. Журнал “Монитор” 1995
14. Основы информационной безопасности/ Галатенко В.А. Под редакцией члена корреспондента РАН В.Б. Бетелина/ М.: ИНТУИТ.РУ “Интернет-Университет Информационных Технологий”, 2003. – 280 с.
15. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. Санкт-Петербург 2007 – 304с
16. Нильс Фергюсон, Брюс Шнайер. Практическая криптография. Москва 2005 – 421с

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

Программу
составила:
старший преподаватель кафедры ВИТ _____М.Д.Романова

Рецензент _____Д.Б.Николаев

Согласовано:

Зав. кафедрой ВИТ _____ В.С.Холушкин

Руководитель ОП _____ В.С.Холушкин