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

# КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
наименование дисциплины

| | |
|---|---|
| Направление подготовки (специальность) | 01.03.02 Прикладная математика и информатика |
| Наименование образовательной программы | Высокопроизводительные вычисления и технологии параллельного программирования |
| 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 201____/201___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/ |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 16 | 2 | 72 | 16 | - | 16 | 40 | - | З |
| **ИТОГО** | **16** | **2** | **72** | **16** | **-** | **16** | **40** | **-** | |

## АННОТАЦИЯ

Курс посвящен изучению теоретических и практические основ защиты информации, знакомство с программно-аппаратными средствами, изучение основных приемов построения программных систем защиты информации. Изучаются способы и методы защиты информации для решения прикладных задач в различных предметных областях.

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ 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 ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Компьютерная безопасность» является базовой (общепрофессиональной) частью профессиональной компетенции и базируется на таких дисциплинах как, «Информатика», «Информационные технологии», «Алгоритмические языки», «Языки и методы программирования».

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

**Профессиональные компетенции в соответствии с задачами и объектами (областями знаний) профессиональной деятельности:**

| Задача профессиональной деятельности (ЗПД) | Объект или область знания | Код и наименование профессиональной компетенции | Код и наименование индикатора достижения профессиональной компе- |
|---|---|---|---|

| | | | |
|---|---|---|---|
| | | | **тенции** |
| **Типы задач профессиональной деятельности: проектный** | | | |
| разработка и реализация проектов, связанных с применением прикладной математики и информатики в конкретных предметных областях | математическое моделирование и высокопроизводительные вычисления в задачах механики сплошной среды и физики высоких плотностей энергии; разработка прикладных программных комплексов; разработка высокопроизводительных ЭВМ и программного обеспечения для них; компьютерное сопровождение и обработка результатов физических экспериментов | **ПК-5** способен к разработке, реализации и оценке проектов научно- исследовательской и инновационной направленности *Основание:* Профессиональный стандарт «40.011Специалист по научно-исследовательским и опытно-конструкторским разработкам» | **З-ПК-5** знать принципы оценки научно исследовательских проектов при проведении их экспертизы; **У-ПК-5** уметь проводить разработку и экспертизу научно-исследовательских проектов; **В-ПК-5** владеть навыками разработки и экспертизы научно-исследовательских проектов; |

**Профессиональные компетенции в соответствии с задачами и объектами (областями знаний) профессиональной деятельности:**

| **Задача профессиональной деятельности (ЗПД)** | **Объект или область знания** | **Код и наименование профессиональной компетенции** | **Код и наименование индикатора достижения профессиональной компетенции** |
|---|---|---|---|
| **Типы задач профессиональной деятельности: производственно-технологический** | | | |
| использование высокопроизводительных вычислений, компьютерных систем и сетей, электронных баз данных в научно-исследовательских, опытно-конструкторских, производственно-технологических работах | математическое моделирование и высокопроизводительные вычисления в задачах механики сплошной среды и физики высоких плотностей энергии; разработка прикладных программных комплексов; разработка высокопроизводительных ЭВМ и программного | **ПК-5.1** Способен разрабатывать математические модели физических процессов и проводить оценку области их применимости *Основание:* Профессиональный стандарт «25.048. Инженер-исследователь по прочности | **З-ПК-5.1** знать Принципы построения математических моделей в различных разделах современной физики, основные законы и точно решаемые задачи в физике **У-ПК-5.1** уметь Выделять главные факторы; уметь определять область применимости математиче- |

| | | | |
|---|---|---|---|
| | обеспечения для них; компьютерное сопровождение и обработка результатов физических экспериментов | летательных аппаратов в ракетно-космической технике при силовом и температурном воздействиях» | ской модели **В-ПК-5.1** владеть навыками оценки вклада параметров, слабо влияющих на поведение моделируемых процессов; навыками валидации разработанных моделей |

## 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** | | **16** | **40** | | |
| **Семестр 1** | | | | | | | | |
| **Раздел 1.** | | | | | | | | |
| 1.1. | Тема 1 Основные понятия, уровни информационной безопасности, составные части системы защиты информации (СЗИ). Проблемы безопасности программного обеспечения. Угрозы информационным ресурсам | **1,2** | **2** | | **2** | **6** | **УО Защита ЛР** | **8** |
| 1.2 | Тема 2. Методы и средства защиты информации Идентификация и аутентификация пользователя в системах управления доступом. Модели систем управления доступом | **3-5** | **2** | | **2** | **6** | **УО Защита ЛР** | **4** |
| **Раздел 2.** | | | | | | | | |

| № 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 | | 16 | 40 | | |
| 2.1 | Тема 1. СЗИ с принудительным назначением паролей. Виды и надежность паролей. Биометрические методы идентификации пользователя | 6-8 | 2 | | 2 | 10 | УО Защита ЛР | 4 |
| 2.2 | Тема 2. Компьютерная стеганография Криптографические методы и средства защиты информации. | 9-10 | 2 | | 2 | 10 | УО Защита ЛР | 8 |
| | **Рубежный контроль** | 11 | | | | | СР | 4 |
| **Раздел 3.** | | | | | | | | |
| 3.1 | Тема 1. Государственные стандарты - алгоритмы шифрования DES и RSA, ГОСТ-28147-89. Хэширование: пароли, ключи, ЭЦП | 12-13 | 4 | | 4 | 10 | УО Защита ЛР | 6 |
| 3.2 | Тема 2. Защита операционных систем. Защита электронного документооборота. Защита от вирусов. Защита от хакеров. Правовое обеспечение защиты информации ограниченного доступа | 14-15 | 4 | | 4 | 10 | УО Защита ЛР | 5 |
| | **Рубежный контроль** | 16 | | | | | СР | 10 |
| | **Промежуточная аттестация** | | | | | З | - | 50 |
| | **Посещаемость** | | | | | | | 5 |
| | **Итого:** | | 16 | | 16 | 40 | - | 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 |
|---|---|---|
| **Раздел 1** | | |
| 1.1 | Тема 1 Основные понятия, уровни информационной безопасности, составные части системы защиты информации (СЗИ). Проблемы безопасности программного обеспечения. Угрозы информационным ресурсам | 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.<br>Основные определения и критерии классификации угроз; действия, приводящие к неправомерному хищению или искажению конфиденциальной информации; наиболее распространенные угрозы доступности; основные угрозы целостности; основные угрозы конфиденциальности. |
| 1.2 | Тема 2. Методы и средства защиты информации Идентификация и аутентификация пользователя в системах управления доступом. Модели систем управления доступом | **.** 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.<br>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. Биометрические методы идентификации пользователя | 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<br>Группы биометрических параметров, предъявляемых пользователем. Биометрические системы защиты информации и оценка их качества. Наиболее распространенные и наиболее надежные биометрические системы, сферы их применения. |
| 2.2 | Тема 2. Компьютерная стеганография Криптографические методы и средства защиты информации. | 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.<br>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 криптосистемы с открытым ключом. Схема электронно-цифровой подписи (ЭЦП). Криптографичекие хэш-функции. |
| **Раздел 3** | | |
| 3.1 | Тема 1. Государственные стандарты - алгоритмы шифрования DES и RSA, ГОСТ-28147-89. Хэширование: пароли, ключи, ЭЦП | 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, про- |

| | | |
|---|---|---|
| | | странство ключей, слабые ключи.<br>Государственные стандарты - алгоритм шифрования ГОСТ-28147-89. Надежность алгоритма, схема преобразования на примере одного раунда. Влияние длины ключа на надежность криптосистем.<br>Хэширование. Понятие односторонней или необратимой функции. Требования к хэш-функции. Пример алгебраических хэш-функций. Пример блочного хэша. Современные системы хэширования: семейство MD4/MD5. |
| 3.2 | Тема 2. Защита операционных систем. Защита электронного документооборота. Защита от вирусов. Защита от хакеров. Правовое обеспечение защиты информации ограниченного доступа | 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.<br>Определение информации, подлежащей защите. Защита 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

| № | Примерные темы 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 обязатель- |

| | |
|---|---|
| | ным 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, курсовых работ;
- подготовка к тестированию, контрольным работам, написанию рефератов;
- подготовка к зачету, экзаменам.

Форма контроля: отчет по лабораторным работам и их защита, защита курсовых работ.

**Учебно-методические пособия:**


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/


**5.**

## 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 |
|---|---|---|---|---|
| 1 | Тема 1 Основные понятия, уровни информационной безопасности, составные части системы защиты информации (СЗИ). Проблемы безопасности программного обеспечения. Угрозы информационным ресурсам | ПК-5,ПК-5.1 | З-ПК-5;У-ПК-5;В-ПК-5<br>З-ПК-5.1;У-ПК-5.1;В-ПК-5.1 | УО2<br>Защита ЛР2 |
| | Тема 2. Методы и средства защиты информации<br>Идентификация и аутентификация пользователя в системах управления доступом. Модели систем управления доступом | ПК-5,ПК-5.1 | З-ПК-5;У-ПК-5;В-ПК-5<br>З-ПК-5.1;У-ПК-5.1;В-ПК-5.1 | УО5<br>Защита ЛР5 |
| 2 | Тема 1. СЗИ с принудительным назначением паролей. Виды и надежность паролей. Биометрические методы идентификации пользователя | ПК-5,ПК-5.1 | З-ПК-5;У-ПК-5;В-ПК-5<br>З-ПК-5.1;У-ПК-5.1;В-ПК-5.1 | УО8<br>Защита ЛР8 |
| | Тема 2. Компьютерная стеганография Криптографические методы и средства защиты информации. | ПК-5,ПК-5.1 | З-ПК-5;У-ПК-5;В-ПК-5<br>З-ПК-5.1;У-ПК-5.1;В-ПК-5.1 | УО10<br>Защита ЛР10 |
| **Рубежный контроль** | | ПК-5,ПК-5.1 | З-ПК-5;У-ПК-5;В-ПК-5<br>З-ПК-5.1;У-ПК-5.1;В-ПК-5.1 | СР11 |
| 3 | Тема 1. Государственные стандарты - алгоритмы шифрования DES и RSA, ГОСТ-28147-89. Хэширование: пароли, ключи, ЭЦП | ПК-5,ПК-5.1 | З-ПК-5;У-ПК-5;В-ПК-5<br>З-ПК-5.1;У-ПК-5.1;В-ПК-5.1 | УО13<br>Защита ЛР13 |
| | Тема 2. Защита операционных систем. Защита электронного документооборота. Защита от вирусов. Защита от хакеров. Правовое обеспечение защиты информации ограниченного доступа | ПК-5,ПК-5.1 | З-ПК-5;У-ПК-5;В-ПК-5<br>З-ПК-5.1;У-ПК-5.1;В-ПК-5.1 | УО15<br>Защита ЛР15 |
| **Рубежный контроль** | | ПК-5,ПК-5.1 | З-ПК-5;У-ПК-5;В-ПК-5<br>З-ПК-5.1;У-ПК-5.1;В-ПК-5.1 | СР16 |
| **Промежуточная аттестация** | | ПК-5,ПК-5.1 | З-ПК-5;У-ПК-5;В-ПК-5<br>З-ПК-5.1;У-ПК-5.1;В-ПК-5.1 | **Зачет** |

## 5.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

### 5.2.1. Оценочные средства для текущего контроля

### 5.2.1.1. Примерные вопросы для устного опроса (УО)

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. Устройства защиты от утечки информации по каналам ПЭМИН.
8. Идентификация и аутентификация пользователя в системах управления доступом.
9. Задачи аутентификации в компьютерных системах.
10. Строгая аутентификация, непрямая, аппаратные и биометрические средства. .
11. СЗИ с принудительным назначением паролей. Виды и надежность паролей.
12. Применение пароля для подтверждения подлинности пользователя.
13. Клавиатурные, электронные, биометрические, смешанные пароли.
14. Требования надежности. Атаки на парольные системы.
15. Администрирование систем управления пользователями, принудительное назначение и смена паролей
16. Биометрические методы идентификации пользователя.
17. Биометрические системы защиты информации и оценка их качества.
18. Компьютерная стеганография.
19. Обзор традиционных методов стеганографии, их классификация.
20. Компьютерная реализация: использование особенностей файловой системы; использование избыточности, присущей файлам формата multi-media.
21. Криптографические методы и средства защиты информации. Исторические этапы становления современной криптографии.
22. Модели криптографии К. Шеннона; теоретико-информационные оценки стойкости симметричных криптосистем с секретным ключом; потоковые шифры; блочные шифры.
23. Шифрование (кодирование) исходных текстов одним ключом по различным криптоалгоритмам.

24. Схема электронно-цифровой подписи (ЭЦП). Криптографические хэш-функции.
25. Государственные стандарты - алгоритмы шифрования DES и RSA.
26. Блочные симметричные криптосистемы с секретным ключом.
27. Государственные стандарты - алгоритм шифрования ГОСТ-28147-89..
28. Хэширование.
29. Защита операционных систем.
30. Защита электронного документооборота.
31. Защита от вирусов.
32. Защита от хакеров.

### 5.2.1.2. Примерные темы и вопросы для самостоятельной работы (СР)

- Виды паролей и их надежность
- Атаки на пароли методом прямого перебора
- Нестандартные пароли
- Электронные ключи
- Надежность биометрических идентификаторов
- Простейшие криптоалгоритмы
- Комплексные СЗИ
- Правила и требования безопасности в организации и на предприятитехнологии, сферы их применения и перспективы развития.

## 5.2.2. Оценочные средства для рубежного контроля

### 5.2.2.1. Примерные задания для решения задач по заданной теме

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

### 5.2.3. Оценочные средства для промежуточной аттестации

### 5.2.3.1. 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:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоения 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>3 – «удовлетворитель-</td><td>Оценка «удовлетворительно» вы-</td></tr>
</table>

| | | | |
|---|---|---|---|
| 60-64 | *но*» | E | ставляется 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. |
| 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 ДИСЦИПЛИНЫ

### 6.1. 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 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 ФОС ВО по «Прикладная математика и информатика» 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

Предлагается

- 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 01.03.02 Прикладная математика и информатика

Автор(ы) _____ М.Д.Романова

Рецензенты _____ В.С.Холушкин

Согласовано:

Зав. кафедрой ВИТ _____ В.С.Холушкин

Руководитель ОП _____ Р.М.Шагалиев