МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## Информационная безопасность и защита информации

Кафедра дифференциальных уравнений и функционального анализа
факультет математики и компьютерных наук

Образовательная программа

01.03.02 Прикладная математика и информатика

Направление (профиль) программы
Математическое моделирование и вычислительная математика

Уровень высшего образования
бакалавриат

Форма обучения
очная

Статус дисциплины: входит в часть ОПОП формируемую участниками
образовательных отношений

Махачкала - 2021

Рабочая программа дисциплины «Информационная безопасность и защита информации» составлена в 2021 году в соответствии с требованиями ФГОС ВО по направлению подготовки

01.03.02 - Прикладная математика и информатика
Приказ № 9 Минобрнауки России от 10.01.2018 г.

Разработчик: кафедра дифференциальных уравнений и функционального анализа, Ибрагимов Мурад Гаджиевич, к. ф.-м. н., доцент.

Рабочая программа дисциплины одобрена:
на заседании кафедры дифференциальных уравнений и функционального анализа от «14» 05 2021 г., протокол №10.

Зав. кафедрой _____ Сиражудинов М.М.

и
на заседании Методической комиссии факультета математики и компьютерных наук от «23» 06 2021 г., протокол №6.

Председатель _____ Бейбалаев В.Д.

Рабочая программа дисциплины согласована с учебно-методическим управлением «9» 07 2021 г.

Начальник УМУ _____ Гасангаджиева А.Г.

# Аннотация рабочей программы дисциплины

Дисциплина «Информационная безопасность и защита информации» входит в часть ОПОП формируемую участниками образовательных отношений бакалавриата по направлению 01.03.02 - Прикладная математика и информатика.
Дисциплина реализуется на факультете математики и компьютерных наук кафедрой дифференциальных уравнений и функционального анализа.

Дисциплина «Информационная безопасность и защита информации» призвана содействовать знакомству студентов с компьютерными телекоммуникациями и возможными подходами к разработке гипертекстовых документов, предназначенных для публикации в глобальной компьютерной сети Internet. Она важна с той точки зрения, что позволяет развивать способности студентов, связанные с общей культурой работы в глобальной сети. Общая проблема информационной безопасности информационных систем; защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение); организационное обеспечение информационной безопасности; защита информации от несанкционированного доступа; математические и методические средства защиты; компьютерные средства реализации защиты в информационных системах; программа информационной безопасности России и пути ее реализации.
Для полноценного усвоения учебного материала по дисциплине "Информационная безопасность и защита информации" студентам необходимо иметь прочные знания по технологии программирования, теории вычислительных сетей, информационным технологиям. Курс закрепляет навыки работы с текстом и графикой, а также навыков программирования и проектирования и разработки информационных систем, являясь, таким образом, прямым продолжением курсов «Информатика и программирование», «Информационные технологии», «Объектно-ориентированное программирование», «Базы данных», «Информационные системы», «Проектирование информационных систем» и многих других.
Рабочая программа дисциплины способствует решению следующих типовых задач учебно-профессиональной деятельности: осуществление процесса обучения принципам построения и эффективного применения информационных систем, операционных оболочек, обслуживающих сервисных программ в соответствии с образовательной программой; организация самостоятельной работы и внеурочной деятельности студентов.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных – ОПК-4, ОПК-5, профессиональных – ПК-3, ПК-4, ПК-5.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, практические занятия, самостоятельная работа.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме контрольная работа, коллоквиум и промежуточный контроль в форме зачета и экзамена.

Объем дисциплины **3** зачетных единиц, в том числе в академических часах по видам учебных занятий 108 ч

Объем дисциплины в очной форме

| Семестр | Учебные занятия | | | | | | | | Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен) |
|---|---|---|---|---|---|---|---|---|---|
| | в том числе | | | | | | | | |
| | Всего | Контактная работа обучающихся с преподавателем | | | | | КСР | СРС, в том числе экз. | |
| | | Всего | из них | | | | | | |
| | | | Лекции | Лабораторные занятия | Практические занятия | консультации | | | |
| 8 | 108 | 48 | 16 | 16 | 16 | - | - | 60 | зачет |

**1. Цели освоения дисциплины**

Цель изучения дисциплины состоит в формировании системного базового представления, умения и навыков студентов по основам информационной безопасности и защите информации, достаточных для последующей эксплуатации автоматизированных систем (АС) и сетей отраслей. Основными целями преподавания дисциплины являются:

- изучение методов построения технических средств защиты объектов и информации;
- изучение методов защиты автоматизированных систем обработки данных от несанкционированного доступа к информации;
- изучение математических и методических средств защиты;
- изучение законодательных мер по защите информации.

Целью курса является освоение практических приемов информационной безопасность и защиты информации. В лекционной части курса рассматриваются общие принципы информационной безопасности и защиты информации. Изучение всех тем сопровождается иллюстрирующими примерами. Лабораторные работы в компьютерных классах служат для индивидуальной работы студентов над учебными задачами и итоговым проектом с целью выработки и закрепления практических навыков информационной безопасности и защиты информации.

Задачи курса - овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности и освоение системных комплексных методов защиты предпринимательской информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения. Изучаемые вопросы рассматриваются в широком диапазоне современных проблем и затрагивают предметные сферы защиты как документированной информации (на бумажных и технических носителях), циркулирующей в традиционном или электронном документообороте, находящейся в компьютерных системах, так и недокументированной информации, распространяемой персоналом в процессе управленческой (деловой) или производственной деятельности.

Перечень дисциплин и тем, усвоение которых студентами необходимо для изучения данной дисциплины. Для полноценного усвоения учебного материала по дисциплине "Информационная безопасность и защита информации" студентам необходимо иметь прочные знания по технологии программирования, теории вычислительных сетей, информационным технологиям, нормы государственного стандарта, общая проблема информационной безопасности информационных систем; защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение); организационное обеспечение информационной безопасности; защита информации от несанкционированного доступа; математические и методические средства защиты; компьютерные средства реализации защиты в информационных системах; программа информационной безопасности России и пути ее реализации.

Основные задачи курса. В процессе обучения студенты должны изучить правовую базу информационной безопасности информационных систем, угрозы информационной безопасности корпоративных систем отраслей, методы защиты информации, включая криптографические, способы защиты информации от несанкционированного доступа к информации и техническим ресурсам корпоративных сетей отраслей, архитектуру и методы организации систем защиты информации. Это достигается с помощью лекций и выполнения лабораторных работ, а также самоподготовки студентов.

## 2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина «Информационная безопасность и защита информации» входит в часть ОПОП формируемую участниками образовательных отношений бакалавриата, по направлению 01.03.02 - Прикладная математика и информатика.

Ядро курса составляют темы, посвященные концепции национальной безопасности и доктрине информационной безопасности, комплексу межотраслевых законодательных актов в сфере правовой защиты информации, формированию и использованию государственной тайны и системе тайн, касающихся информации ограниченного доступа; сущности конфиденциального делопроизводства. Изучение означенных тем является обязательным. Особого внимания заслуживает тема государственной тайны, предусматривающая наиболее серьезную уголовную ответственность, а также темы коммерческой тайны и интеллектуальной собственности, как наиболее актуальные в рыночных условиях. Тема доктрины информационной безопасности важна не только тем, что раскрывает сущность данного вопроса, но и показывает взгляд государства на состояние и обеспечение информационной безопасности государства, общества и граждан. Не меньшее внимание следует уделить в рыночных условиях теме организации защищенного документооборота, когда конфиденциальная информация становится конкурентным преимуществом на рынке.

## 3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения)

| **Код и наименование компетенции из ОПОП** | **Код и наименование индикатора достижения компетенций** | **Планируемые результаты обучения** | **Процедура освоения** |
|---|---|---|---|
| ОПК-4. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач | ОПК-4.1.Знает основные положения и концепции прикладного и системного программирования, архитектуры | Знает: основные принципы документационного обеспечения профессиональной деятельности с учетом требований информационной | Конспектирование и проработка лекционного материала. Участие в практических занятиях. Самостоятельная |

| | | | |
|---|---|---|---|
| профессиональной деятельности | компьютеров и сетей (в том числе и глобальных). | безопасности; алгоритмы решения стандартных организационных задач; основные понятия, теоретические положения и методы программирования на языках высокого уровня. Умеет: применять методы программирования при решении разнообразных задач теоретического и практического содержания. Владеет: методами программирования на различных языках высокого уровня для решения теоретических и практических задач. | работа. |
| | ОПК-4.2.Умеет использовать информационные технологии в профессиональной деятельности. | Знает: основные направления применения информационно коммуникационных технологий в науке и образовании; принципы построения сетей; локальные и глобальные сети; сеть Интернет; безопасность компьютерных сетей. Умеет: выбирать эффективные информационные технологии для использования в научных исследованиях и учебном процессе. Владеет: методами математического и алгоритмического моделирования и информационно коммуникационных технологий в науке и образовании. | |
| | ОПК-4.3.Имеет практические навыки разработки программного обеспечения для решения зада | Знает: теоретические положения и методы программирования на языках высокого уровня. Умеет: выбирать эффективные | |

| | | | |
|---|---|---|---|
| | профессиональной деятельности. | информационные технологии для использования в научных исследованиях и учебном процессе. Владеет: навыками построения алгоритмов и программ различных явлений и процессов, навыками использования информационных технологий для обработки данных. | |
| ОПК-5. Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения | ОПК-5.1.Знает основные современные языки программирования, технологии создания и эксплуатации программных продуктов и программных комплексов. | Знает: основные принципы документационного обеспечения профессиональной деятельности с учетом требований информационной безопасности; алгоритмы решения стандартных организационных задач; основные понятия, теоретические положения и методы программирования на языках высокого уровня. Умеет: применять методы программирования при решении разнообразных задач теоретического и практического содержания. Владеет: методами программирования на различных языках высокого уровня для решения теоретических и практических задач. | Конспектирование и проработка лекционного материала. Участие в практических занятиях. Самостоятельная работа. |
| | ОПК-5.2.Умеет разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения. | Знает: основные направления применения информационно коммуникационных технологий в науке и образовании; принципы построения сетей; локальные и глобальные сети; сеть Интернет; безопасность компьютерных сетей. | |

| | | | |
|---|---|---|---|
| | | Умеет: выбирать эффективные информационные технологии для использования в научных исследованиях и учебном процессе. Владеет: методами математического и алгоритмического моделирования и информационно коммуникационных технологий в науке и образовании. | |
| | ОПК-5.3.Имеет практические навыки разработки программного обеспечения. | Знает: теоретические положения и методы программирования на языках высокого уровня. Умеет: выбирать эффективные информационные технологии для использования в научных исследованиях и учебном процессе. Владеет: навыками построения алгоритмов и программ различных явлений и процессов, навыками использования информационных технологий для обработки данных. | |
| ПК-3. Способен вести педагогическую деятельность по проектированию и реализации образовательного процесса в образовательных организациях дошкольного, начального общего, основного общего, среднего общего образования | ПК-3.1. Знает требования к организационно-методическому и педагогическому обеспечению программ общего образования, среднего профессионального образования и дополнительных профессиональных программ; знает методические основы преподавания дисциплин математики и | Знает: образовательный стандарт и программы среднего общего образования, среднего профессионального образования и дополнительные общеобразовательные и профессиональные программы соответствующего уровня; методические основы преподавания дисциплин математики и информатики. Умеет: профессионально грамотно пользоваться организационно-методическим и учебно- | Конспектирование и проработка лекционного материала. Участие в практических занятиях. Самостоятельная работа. |

| | | | |
|---|---|---|---|
| | информатики. | методическим обеспечением образовательной программы соответствующего уровня. Владеет: психолого-педагогическими и методическими основами преподавания дисциплин математики и информатики. | |
| | ПК-3.2. Умеет планировать занятия по программам обучения математике и информатике с учетом уровня подготовки и психологии аудитории. | Знает: на достаточно высоком уровне учебные курсы математики и информатики в рамках программы соответствующего уровня. Умеет: оценивать объем материала, необходимого для освоения того или иного программного вопроса в области математики и информатики; устанавливать связи между различными предметными разделами с учетом уровня подготовки и психологии данной аудитории. Владеет: достаточной информацией о современном состоянии развития различных областей математики и информатики и об актуальных вопросах преподавания математики и информатики. | |
| | ПК-3.3. Имеет практический опыт проведения уроков и индивидуальных занятий по математике и информатике. | Знает: разные подходы к определению основных понятий математики; основные понятия информатики; формулировки математических утверждений при различных изменениях их исходных условий; различные языки программирования. | |

| | | | |
|---|---|---|---|
| | | Умеет: оценивать объем материала, необходимого для освоения того или иного программного вопроса по математике и информатике. Владеет: методикой изложения основного материала того или другого раздела математики и информатики по программе данной образовательной организации. | |
| ПК-4. Способен к преподаванию по программам профессионального обучения, среднего профессионального образования (СПО) и дополнительным профессиональным программам (ДПП), ориентированным на соответствующий уровень квалификации | ПК-4.1. Выполняет все требования к организационно-методическому и организационно-педагогическому обеспечению основных и дополнительных образовательных программ | Знает: на достаточно высоком уровне курсы математики и информатики, а также современные направления развития образовательных технологий. Умеет: профессионально оценивать объем материала, достаточного для организационно методического и учебно-методического обеспечения образовательной программы соответствующего уровня. Владеет: достаточной информацией о современном состоянии развития различных областей математики и информатики и об актуальных вопросах преподавания математики и информатики. | Конспектирование и проработка лекционного материала. Участие в практических занятиях. Самостоятельная работа. |
| | ПК-4.2. Планирует урочную деятельность и внеклассные мероприятия на основе существующих методик в зависимости от уровня | Знает: современные методы проведения учебных занятий и внеклассных мероприятий, в том числе активные и интерактивные методы. Умеет: планировать данный урок или внеклассное мероприятие | |

| | | | |
|---|---|---|---|
| | квалификации. | с выбором разнообразных методик. Владеет: навыками составления поурочных планов и планов внеклассных мероприятий на основе существующих методик. | |
| | ПК-4.3. Выбирает оптимальные методы и методики преподавания при планировании занятия. | Знает: различные методы проведения учебных занятий и внеклассных мероприятий. Умеет: планировать данное занятие или внеклассное мероприятие с выбором оптимального метода или методики преподавания. Владеет: навыками планирования уроков на основе активных и интерактивных методик | |
| ПК-5. Способен к анализу требований к программному обеспечению | ПК-5.1. Знает методы анализа возможностей реализации требований к программному обеспечению | Знает: методы структурного анализа требований к программному обеспечению Умеет: применять методы разработки и исследования математических, информационных и имитационных моделей по тематике выполняемых прикладных работ. Владеет: навыками разработки и исследования алгоритмов, протоколов, вычислительных моделей и баз данных для реализации функций и сервисов систем информационных технологий. | Конспектирование и проработка лекционного материала. Участие в практических занятиях. Самостоятельная работа. |
| | ПК-5.2. Умеет использовать возможности существующей программно-технической архитектуры, методологию | Знает: общие вопросы теории интеллектуальных систем, различные методы обработки информации, способы их программной реализации. Умеет: применять | |

| | | | |
|---|---|---|---|
| | разработки программного обеспечения и технологии программирования | современные системные программные средства, технологии и инструментальные средства Владеет: основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления информацией; у. | |
| | ПК-5.3. Имеет практический опыт проведения оценки и обоснование рекомендуемых решений | Знает архитектуру современных высокопроизводительных вычислительных систем Умеет обеспечивать передачу информации между приложениями Владеет навыками разработки проектной и программной документации; методикой разработки архитектуры, алгоритмических и программных решений системного и прикладного программного обеспечения. | |

## 4. Объем, структура и содержание дисциплины

4.1. Объем дисциплины составляет 6 зачетных единиц, 216 академических часов.

### 4.2. Структура дисциплины

| № п/п | Разделы и темы дисциплины | Семестр | Неделя семестра | Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах) | | | | | Формы текущего контроля |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Всего | Лекции | Практич. занятия | Лаборатор. занятия | СРС | |
| 1 | **Модуль 1** | | | | | | | | |
| 2 | **Тема 1.** Предмет, цели и задачи дисциплины | 8 | 1 | 12 | 2 | 2 | 2 | 6 | Устный опрос, |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | «Информационная безопасность и защита информации». Основные определения и понятия. Законодательство в области информационной безопасности и защиты данных. Структуры и нормативные акты, их направления. | | | | | | | | письменная контрольная работа, лабораторная работа. |
| 3 | **Тема 2.** Классификация информационных ресурсов, характеристика и основные свойства. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа. Классификация и анализ угроз информационной безопасности корпоративным системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический. | 8 | 2 | 12 | 2 | 2 | 2 | 6 | |
| 4 | **Тема 3.** Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блоковые и поточные шифры. Стойкость криптосистем. Американский стандарт шифрования данных DES. Отечественный стандарт криптографической защиты ГОСТ 28147-89. Асимметричные криптосистемы. Математические основы криптографии с открытым ключом. Криптосистема RSA. Криптосистема Эль Гамаля. Криптосистемы | 8 | 3 | 12 | 2 | 2 | 2 | 6 | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | без передачи ключей. Управление ключами. Методы генерации, хранения и распределения ключей. Протоколы управления ключами. | | | | | | | | |
| 5 | **Итого по модулю 1:** | **8** | **1-3** | **36** | **6** | **6** | **6** | **18** | Коллоквиум |
| 6 | **Модуль 2** | | | | | | | | |
| 7 | **Тема 4.** Аппаратно-программные решения защиты информации в информационных системах. Электронные замки. Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись (ЭЦП). Однонаправленная хэш-функция. Идентификация и аутентификация объектов сети. Идентификация и подтверждение подлинности пользователей сети. | 8 | 4 | 18 | 2 | 2 | 2 | 12 | Устный опрос, письменная контрольная работа, лабораторная работа. |
| 8 | **Тема 5.** Математические методы обеспечения защиты от несанкционированного доступа и конфиденциальности. Криптография: понятия, подходы, направления исследований. | 8 | 5 | 18 | 2 | 2 | 2 | 12 | |
| 9 | **Итого по модулю 2:** | **8** | **4-5** | **36** | **4** | **4** | **4** | **24** | Коллоквиум |
| 10 | **Модуль 3** | | | | | | | | |
| 11 | **Тема 6.** Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ. Особенности межсетевого экранирования на различных уровнях модели OSI. Криптография и криптоанализ в | 8 | 6 | | 2 | 2 | 2 | 6 | Устный опрос, письменная контрольная работа, лабораторная работа. |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | авторизации, аутентификации и в обмене информации. Основные понятия и принципы криптографии. Особенности реализация криптографических методов. | | | | | | | | |
| 12 | **Тема 7.** Средства антивирусной защиты. Классификация вирусов и средств защиты. Виды антивирусных программных продуктов. Характеристика наиболее популярных антивирусных пакетов. Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ. | 8 | 7 | | 2 | 2 | 2 | 6 | |
| 13 | **Тема 8.** Информационная безопасность в глобальном информационном пространстве Интернет. Безопасная интеграция в Интернет. Программные и технологические решения. Угрозы и риски интернет-технологий. Стандартизация информационной безопасности в Интернет. Программно-аппартные технологии Интернет. Основные понятия и принципы криптографии. Особенности реализация криптографических методов. | 8 | 8 | | 2 | 2 | 2 | 6 | |
| 14 | **Итого по модулю 3:** | **8** | **6-8** | **36** | **6** | **6** | **6** | **18** | Коллоквиум |
| 15 | **Итого за 8 семестр:** | **8** | **1-8** | **108** | **16** | **16** | **16** | **60** | Зачет |
| 16 | **Итого:** | **8** | **1-8** | **108** | **16** | **16** | **16** | **60** | **Зачет** |

**4.3. Содержание дисциплины, структурированное по темам (разделам)**
**4.3.1. Содержание лекционных занятий по дисциплине**

**8 семестр**

**Модуль 1**

**Лекция 1.** Предмет, цели и задачи дисциплины «Информационная безопасность и защита информации». Основные определения и понятия.

Законодательство в области информационной безопасности и защиты данных. Структуры и нормативные акты, их направления.

План-вопросы:

1. Классификация нормативных актов в области ИБ и ЗД;
2. Государственные органы, регулирующие вопросы информационной безопасности;
3. Классификация информации по степени ее защиты;
4. Доктрина информационной безопасности РФ;
5. Законодательство и нормативные акты Российской Федерации.

**Лекция 2.** Классификация информационных ресурсов, характеристика и основные свойства. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа.

Классификация и анализ угроз информационной безопасности корпоративным системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический.

**Лекция 3.** Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блоковые и поточные шифры. Стойкость криптосистем. Американский стандарт шифрования данных DES. Отечественный стандарт криптографической защиты ГОСТ 28147-89.

Асимметричные криптосистемы. Математические основы криптографии с открытым ключом. Криптосистема RSA. Криптосистема Эль Гамаля. Криптосистемы без передачи ключей. Управление ключами. Методы генерации, хранения и распределения ключей. Протоколы управления ключами.

**Модуль 2**

**Лекция 4.** Аппаратно-программные решения защиты информации в информационных системах.

План-вопросы:

1. Аппаратно-программные средства контроля доступа
1.1. iButton.
1.2 Смарт-карты.
1.3. Устройства ввода на базе USB-ключей.
1.4. Proximity.
1.5. Биометрические УВИП
1.6. Комбинированные устройства ввода.
2. Электронные замки.

Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись (ЭЦП). Однонаправленная хэш-функция.

Идентификация и аутентификация объектов сети. Идентификация и подтверждение подлинности пользователей сети.

**Лекция 5.** Математические методы обеспечения защиты от несанкционированного доступа и конфиденциальности.

План-вопросы:

1. Исторический очерк развития криптографии
1.1. Криптография древнего периода.
1.2. Криптография арабского мира.
1.3. Криптография в эпоху Возрождения (XIV-XVI вв.).
1.4. Криптография в XVII-XVIII веках.
1.5. Криптография в XIX веке.
1.6. Криптография в XX веке.
1.7. О криптографии нового времени.
2. Криптография: понятия, подходы, направления исследований.
2.1 Предисловие.
2.2. Базовая терминология.
2.3. Основные алгоритмы шифрования.
2.4. Цифровые подписи.
2.5. Криптографические хэш-функции.
2.6. Криптографические генераторы случайных чисел.
2.7. Обеспечиваемая шифром степень защиты.
2.8. Криптоанализ и атаки на криптосистемы.

## Модуль 3

**Лекция 6.** Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ. Особенности межсетевого экранирования на различных уровнях модели OSI.

Криптография и криптоанализ в авторизации, аутентификации и в обмене информации.

План–вопросы:

1. Основные понятия и принципы криптографии.
1.1 Симметричные криптосистемы.
1.2 Асимметричные криптосистемы.
1.3 Электронная цифровая подпись.
1.4 Управление ключами в криптографических системах защиты информации.
2. Особенности реализация криптографических методов.
2.1 Федеральная инфраструктура открытых ключей.
2.2 Направления исследований в области криптосистем.

**Лекция 7.** Средства антивирусной защиты. Классификация вирусов и средств защиты. Виды антивирусных программных продуктов. Характеристика наиболее популярных антивирусных пакетов.

Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ.

**Лекция 8.** Информационная безопасность в глобальном информационном пространстве Интернет. Безопасная интеграция в Интернет. Программные и технологические решения.

План-вопросы:

1. Угрозы и риски интернет-технологий.
2. Стандартизация информационной безопасности в Интернет.
3. Программно-аппартные технологии Интернет.

3.1 Брандмауэры.

3.2 Программное обеспечение защиты информации в Интернет.

4 Основные понятия и принципы криптографии.

4.1 Симметричные криптосистемы.

4.2 Асимметричные криптосистемы.

4.3 Электронная цифровая подпись.

4.4 Управление ключами в криптографических системах защиты информации.

5. Особенности реализация криптографических методов.

### 4.3.2. Содержание лабораторно-практических занятий по дисциплине 8 семестр

Лабораторные работы в компьютерных классах служат для самостоятельной работы студентов над учебными задачами с целью выработки и закрепления практических навыков по предмету «Информационная безопасность и защита информации».

| **Лабораторная работа** | **Цель и содержание лабораторной работы** | **Результаты лабораторной работы** |
|---|---|---|
| **Модуль1** | | |
| Лабораторная работа 1. Защита баз данных на примере MS ACCESS. | Алгоритм защиты БД MS Access. Порядок выполнения и результаты работы. | Защита на уровне пароля. Защита на уровне пользователя. Создать и изменить пароль. |
| Лабораторная работа 2. Стандартные способы зашиты информации. | О сложности паролей. Защита информации в офисных документах. Защита информации в архивных файлах. Программы «взлома» паролей в офисных документах, архивах. Программы «взлома» паролей в офисных документах, архивах. | Освоить программы паролей файлов офисных приложений и архив. |
| Лабораторная работа 3. Основы криптографической защиты информации. Симметричные алгоритмы. | Криптография. Ключ. Криптоанализ. Кодирование. Симметричные криптосистемы Шифры перестановки. Шифры простой замены. Шифры сложной замены | Процесс шифрования. |

| | | |
|---|---|---|
| Лабораторная работа 4. Основы криптографической защиты информации. Асимметричные алгоритмы. | Асимметричные криптосистемы. Схема шифрования Эль Гамаля. Алгоритм Диффи-Хелмана. Криптосистема шифрования данных RSA. | Процесс шифрования. |
| Лабораторная работа 5. Программное обеспечение защиты информации. | Основные функции ПО. Генерировать ключи шифрования и сохранить их дискете (диске). Зашифровать информацию, используя полученные ключи. Передать информацию (скопировать на другой носитель) защищенную ключом. | Процесс шифрования. |
| Лабораторная работа 6. Хранение сведений о пользователе на сервере. | Создайте уникальный ключ, идентифицирующий пользователя. Сохраните созданный ключ на клиентском компьютере в виде файла cookie. Создайте на сервере файл для хранения сведений о пользователе. Сохраните сведения о пользователе на сервере, используя созданный уникальный ключ в качестве индекса. | Создание уникальных ключей для идентификации пользователей. |
| **Модуль 2** | | |
| Лабораторная работа 7. Создания файлов для хранения сведений о пользователе | В Visual Studio создайте XML-файл, содержащий примерные значения в полях данных, которые предназначены для хранения сведений о пользователе. Сгенерируйте на основе XML-файла схему XML. Схема XML позволяет в наборе данных ссылаться по имени на данные, хранящиеся в XML-файле. Задайте поле ключа в схеме XML, чтобы использовать его с методом Find для поиска записей в наборе данных. Прочитайте содержимое схемы XML и XML-файла в набор данных. | Сохранение сведений пользователе на сервере. Извлечение сведений о пользователе из набора данных. |
| Лабораторная работа 8. Проверка наличия поддержки дополнительных возможностей. | Добавьте к приложению Web-форму с именем Default.aspx и сделайте ее начальной страницей приложения. Добавьте к созданной Web-форме следующий обработчик события Page_Load. | Создание приложения Advanced Features. Готовая Web-форма. |
| Лабораторная работа 9. Аутентификация и авторизация пользователей | Войдите на сервер как администратор. Выберите из меню Start (Пуск) пункт Administrative Tools\Computer Management (Администрирование\Управление компьютером), чтобы запустить консоль Computer Management. Выберите в списке слева элемент Local Users And Groups (Локальные пользователи и группы), затем папку Users, чтобы открыть список авторизованных пользователей для этого компьютера. В списке справа дважды щелкните левой кнопкой анонимную учетную запись с именем в форме IUSER_имя_компътера - оснастка Computer Management откроет окно свойств учетной записи. | Web-форма. |

| | | |
|---|---|---|
| Лабораторная работа 10. Включение аутентификации Windows | Создайте новый проект Web-приложения. Если проект использует Visual Basic-NET, измените элемент, определяющий авторизацию следующим образом (см, строку, выделенную полужирным шрифтом в HTML-коде), а если Visual C# , то следующий элемент необходимо добавить целиком. Добавьте к коду начальной Web-формы проекта следующее HTML-определение таблицы Переключите окно формы в режим Design и добавьте к объекту кода начальной Web-формы следующие строки. | Web-форма. |
| **Модуль 3** | | |
| Лабораторная работа 11. Аутентификация Forms. | В файле Web.config установите режим аутентификации в «Forms». Создайте Web-форму для сбора учетных данных. Создайте файл или БД для хранения имен и паролей пользователей. Напишите код, добавляющий сведения о новых пользователях в файл или БД. Напишите код, выполняющий аутентификацию пользователей с применением файла или БД со сведениями о пользователях. | Web-форма. |
| Лабораторная работа 12. Сохранение сведений о пользователе. | Создайте новую Web-форму и назовите ее Background.aspx. Поместите на Web-форму серверный элемент управления DropDownList, элементы списка которого задают различные цвета фона. Проще всего для этого использовать режим HTML (а не Design), поскольку в нем удается быстро создавать элементы списка путем копирования-вставки соответствующего HTML-кода. Вот HTML-код, определяющий DropDownList и элементы его списка. | Создание Web-формы. |
| Лабораторная работа 13. Сохранение сведений о пользователе. | Измените элемент <body> Web-формы так, чтобы он задавал цвет фона с помощью значений элементов списка DropDownList, используя привязку данных. Вот HTML- код модифицированного элемента <body>: <body bgColor="<%# drpBackground.SelectedItem.Value %>"> . Добавьте к обработчику события Page Load код, проверяющий наличие файла cookie и создающий его, если он не существует. Если cookie существует, этот код задаст цвет фона на основе хранящихся в нем данных. Обработчик события Page Load также использует привязку данных, чтобы обновить цвета фона. | Создание Web-формы. |
| Лабораторная работа 14. Создание Web-формы Mail. | Создайте новую Web-форму и назовите ее Mail.aspx. Добавьте к Web-форме текст и серверные элементы управления, показанные в следующем HTML-коде. | Создание Web-формы. |
| Лабораторная работа 15. Создание Web-формы Mail. | Чтобы применять сокращенные имена в ссылках на члены пространства имен System. Web. Mail, поместите в начало модуля Web-формы следующие операторы: Visual Basic .NET Imports System.Web.Mail Visual C# using System. Web.Mail. | Создание Web-формы. |

| | | |
|---|---|---|
| | Добавьте к обработчику события butSend_Click для создания объекта MailMessage и отправки сообщения с сервера. | |
| Лабораторная работа 16. Создание пользовательского интерфейса на основе фреймов. | Создайте новую HTML-страницу и назовите ее Contents.htm. Добавьте к странице Contents следующие гиперссылки. Добавьте к странице Contents следующий сценарий. Создайте набор фреймов для отображения страниц проекта. Для этого из меню Project выберите команду Add New Item, затем из списка Templates выберите Frameset и при- свойте новому файлу имя Frameset.htm, Щелкните Open - Visual Studio откроет диалоговое окно Select A Frameset Template. Выберите для набора фреймов шаблон Banner And Content и шелкните OK. Visual Studio откроет пустой набор фреймов в окне Design.Щелкните правой кнопкой крайний слева фрейм и выберите из контекстного меню команду Set Page For Frame — Visual Studio откроет диалоговое окно Select Page.В диалоговом окне Select Page укажите файл Contents.htm и щелкните OK, чтобы назначить страницу Contents для отображения в этом фрейме. Назначьте страницу с набором фреймов начальной страницей приложения. Для этого в окне Solution Explorer шелкните правой кнопкой файл Frameset.htm и выберите из контекстного меню команду Set As Start Page. | Создание Web-формы. |

5. **Образовательные технологии**

Сочетание традиционных образовательных технологий в форме лекции с интерактивными семинарскими занятиями и компьютерными автоматизированными информационными технологиями при выполнении лабораторных работ и проведении контрольных мероприятий (экзаменов, зачетов, промежуточного тестирования). Оценка качества освоения материала дисциплины складывается из оценки ответа на экзамене, оценки выполнения практической работы, представляемой на экзамен, оценки полноты и качества конспекта, оценки полноты и качества выполнения заданий на самостоятельную работу.

## 6. Учебно-методическое обеспечение самостоятельной работы студентов

### 6.1. Примерное распределение времени самостоятельной работы студентов

| Вид самостоятельной работы | Примерная трудоёмкость, а.ч. |
|---|---|
| Предмет, цели и задачи дисциплины «Информационная безопасность и защита информации». Основные определения и понятия. Законодательство в области информационной безопасности и защиты данных. Структуры и нормативные акты, их направления. | 6 |

| | |
|---|---|
| Классификация информационных ресурсов, характеристика и основные свойства. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа. Классификация и анализ угроз информационной безопасности корпоративным системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический. | 6 |
| Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блоковые и поточные шифры. Стойкость криптосистем. Американский стандарт шифрования данных DES. Отечественный стандарт криптографической защиты ГОСТ 28147-89.<br>Асимметричные криптосистемы. Математические основы криптографии с открытым ключом. Криптосистема RSA. Криптосистема Эль Гамаля. Криптосистемы без передачи ключей. Управление ключами. Методы генерации, хранения и распределения ключей. Протоколы управления ключами. | 6 |
| Аппаратно-программные решения защиты информации в информационных системах. Электронные замки.<br>Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись (ЭЦП). Однонаправленная хэш-функция.<br>Идентификация и аутентификация объектов сети. Идентификация и подтверждение подлинности пользователей сети. | 12 |
| Математические методы обеспечения защиты от несанкционированного доступа и конфиденциальности.<br>Криптография: понятия, подходы, направления исследований. | 12 |
| Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ. Особенности межсетевого экранирования на различных уровнях модели OSI.<br>Криптография и криптоанализ в авторизации, аутентификации и в обмене информации.<br>Основные понятия и принципы криптографии.<br>Особенности реализация криптографических методов. | 6 |
| Средства антивирусной защиты. Классификация вирусов и средств защиты. Виды антивирусных программных продуктов.<br>Характеристика наиболее популярных антивирусных пакетов.<br>Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ. | 6 |
| Информационная безопасность в глобальном информационном пространстве Интернет. Безопасная интеграция в Интернет. Программные и технологические решения.<br>Угрозы и риски интернет-технологий.<br>Стандартизация информационной безопасности в Интернет.<br>Программно-аппартные технологии Интернет.<br>Основные понятия и принципы криптографии.<br>Особенности реализация криптографических методов. | 6 |
| Итого СРС: | 60 |

**6.2. Виды и порядок выполнения самостоятельной работы**

1. Изучение лекционных материалов (электронные варианты) и рекомендованной литературы.
2. Выполнение индивидуальных заданий на составление программ и подготовка к отчету по ним.
3. Решение задач и упражнений, сформулированных в электронных приложениях к лекции
4. Подготовка к текущему и промежуточному контролю.
5. Подготовка к экзамену.

**6.3. Порядок контроля:**

1. Блиц-опрос на лабораторных занятиях, 2. Проверка выполнения пакета заданий и прием отчета по ним, 3. Текущий контроль за выполнением задач, сформулированных в электронных вариантах к лекции, 4. Промежуточный отчет (коллоквиумы, к.р.), 5. Экзамен.

Текущий контроль включает систематический блиц-опрос и проверку домашнего задания.

Промежуточный контроль проводится в виде отчета по пакетам заданий, предварительная проверка решений практикуется по файлам, отправленным по электронной почте.

Итоговый контроль проводится в виде устного экзамена с обязательным устным собеседованием.

Критерии выставления оценок:

«отлично» - владение теоретическим материалом, возможно, за исключением деталей справочного плана, и наличие навыков решения задач;

«хорошо» - владение разделами «Классификация криптографических методов. Традиционные (симметричные) криптосистемы», «Аппаратно-программные решения защиты информации в информационных системах» «Математические методы обеспечения защиты от несанкционированного доступа и конфиденциальности»;

«удовлетворительно» - знания по разделам «Предмет, цели и задачи дисциплины «Информационная безопасность и защита информации». Основные определения и понятия», «Законодательство в области информационной безопасности и защиты данных», «Структуры и нормативные акты, их направления» и посещение занятий.

Пакет заданий для самостоятельной работы выдается по истечению месяца с начала семестра, определяются предельные сроки их выполнения и сдачи.

## 6.4. Примеры заданий для самостоятельного решения

| Разделы и темы для самостоятельного изучения | Виды и содержание самостоятельной работы |
|---|---|
| **Тема 1.** Криптографические протоколы. | Элементы протоколов. Введение в протоколы. Передача информации с использованием симметричной криптографии. Однонаправленные функции.<br>Однонаправленные хэш-функции Передача информации с использованием криптографии с открытыми ключами. Цифровые подписи и шифрование. Генерация случайных и псевдослучайных последовательностей. |
| **Тема 2.** Основные протоколы | Обмен ключами. Удостоверение подлинности. Формальный анализ протоколов проверки подлинности и обмена ключами. Разделение секрета. Совместное использование секрета. Криптографическая защита баз данных. |
| **Тема 3.** Промежуточные протоколы. | Служба меток времени. Подсознательный канал. Неотрицаемые цифровые подписи. Подписи уполномоченного свидетеля. Подписи по доверенности. Групповые подписи. Подписи с обнаружением подделки.<br>Вычисления с зашифрованными данными. Вручение битов. Подбрасывание «честной» монеты. Мысленный покер. Однонаправленные сумматоры. Раскрытие секретов «все или ничего». Условие вручение ключей. |
| **Тема 4.** Развитые протоколы. | Доказательство с нулевым знанием. Использование доказательства с нулевым знанием для идентификации. Слепые подписи. Личностная криптография с открытыми ключами. Рассеянная передача. Рассеянные подписи. Одновременная подпись контракта. Электронная почта с подтверждением. Одновременный обмен с секретами. |
| **Тема 5.** Эзотерические протоколы. | Безопасные выборы. Безопасные вычисления с несколькими участниками. Анонимная широковещательная передача сообщений. Электронные наличные. |
| **Тема 6.** Длина ключа. | Длина симметричного ключа. Длина открытого ключа. Сравнение длин симметричных и открытых ключей. Какова должна быть длина ключа? |
| **Тема 7.** Управление ключами. | Генераций ключей. Нелинейные пространства ключей. Передача ключей. Проверка ключей. Использование ключей обновление ключей. Хранение ключей. Резервные ключи. Скомпрометированные ключи. Время жизни ключей. Разрушение ключей. Управление открытыми ключами. |

| | |
|---|---|
| **Тема 8.** Типы алгоритмов и криптографические режимы. | Режим электронной шифровальной книги. Повтор блока. Режим сцепления блоков шифра. Потоковые шифры. Самосинхронизирующиеся потоковые шифры. Режим обратной связи по шифру. Синхронные потоковые шифры. Режим выходной обратной связи. Другие режимы блочных шифров. Выбор режима шифра. Блочные шифры против потоковых шифров. |
| **Тема 9.** Математические основы | Теория информации. Теория сложности. Теория чисел. Разложение на множители. Генерации простых чисел. Дискретные логарифмы и конечное поле. |
| **Тема 10.** Стандарт шифрования данных DES. | Описание Jgbcfybt DES. Безопасность DES. Варианты DES. Насколько безопасен сегодня DES. |

## 7. Фонд оценочных средств, для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

### 7.1. Типовые контрольные задания

#### 7.1.1. Темы рефератов:

Основные понятия и принципы криптографии.
Средства антивирусной защиты.
Классификация вирусов и средств защиты.
Виды антивирусных программных продуктов.
Информационная безопасность в глобальном информационном пространстве Интернет.
Угрозы и риски интернет-технологий.
Стандартизация информационной безопасности в Интернет.
Программно-аппартные технологии Интернет.
Основные понятия и принципы криптографии.

#### 7.1.2. Примерные упражнения и задания для текущего контроля

**Примерный перечень контрольных вопросов и заданий**

**Контрольная работа 1**

1. Дать определение информационной безопасности и охарактеризовать ее цели, задачи и структуру.
2. Определить место информационной безопасности в структуре информационного права.
3. Проанализировать современные проблемы информационной безопасности предпринимательской деятельности.
4. Описать порядок охраны информационных ресурсов открытого доступа.
5. Охарактеризовать порядок защиты информационных ресурсов ограниченного доступа.
6. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.

## Контрольная работа 2

1. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.
2. Проанализировать состав показателей (граф и зон) перечня конфиденциальных сведений фирмы, обосновать целевое назначение показателей и их взаимосвязь.
3. Регламентировать в виде фрагмента инструкции порядок доступа персонала к электронным конфиденциальным документам фирмы.
4. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.
5. Обосновать целесообразность состава процедур, сопровождающих автоматизированный учет конфиденциальных документов.
6. Составить графическую схему перемещения электронной и традиционной учетной карточки конфиденциального документа.
7. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения
8. Сравнить способы учета конфиденциальных документов, изготовленных на дискете, выявить критерии определения эффективности каждого из способов.

## Контрольная работа 3

1. Сравнить способы учета электронных конфиденциальных документов, передаваемых по линии защищенной компьютерной связи, выявить критерии определения эффективности каждого из способов.
2. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.
3. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.
4. Проанализировать особенности текста конфиденциального документа.
5. Дать графическую схему расположения специфических реквизитов формуляра конфиденциального документа, описать порядок оформления реквизитов.
6. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.
7. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.
8. Обосновать необходимость реквизитов, указываемых на лицевой и оборотной стороне пакета (конверта) с конфиденциальным документом.
9. Сформулировать возможности, трудности и направления использования электронной почты для передачи конфиденциальных документов.
10. Составить фрагмент номенклатуры дел, содержащих конфиденциальные документы.

**Контрольная работа 4**

1. Регламентировать в виде фрагмента инструкции порядок формировании вдела электронных конфиденциальных документов.
2. Проанализировать задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами.
3. Проанализировать целесообразность, назначение и порядок оформления реквизитов акта об уничтожении документов и дел.
4. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.
5. Проанализировать пути поиска документов и дел, не обнаруженных при проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.
6. Составить план эвакуации и охраны конфиденциальных документов и дел при возникновении угрозы экстремальной ситуации, регламентировав способы обеспечения их сохранности при упаковке и транспортировке документов и дел, не обнаруженных при проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.
7. Составить план эвакуации и охраны конфиденциальных документов и дел при возникновении угрозы экстремальной ситуации, регламентировав способы обеспечения их сохранности при упаковке и транспортировке.

**7.1.3. Вопросы к зачету**

1. Предмет, цели и задачи дисциплины.
2. Основные определения и понятия.
3. Законодательство в области информационной безопасности и защиты данных.
4. Структуры и нормативные акты, их направления».
5. Классификация нормативных актов в области ИБ и ЗД.
6. Государственные органы, регулирующие вопросы информационной безопасности.
7. Классификация информации по степени ее защиты.
8. Доктрина информационной безопасности РФ.
9. Законодательство и нормативные акты Российской Федерации.
10. Классификация информационных ресурсов, характеристика и основные свойства.
11. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа.
12. Классификация и анализ угроз информационной безопасности корпоративным системам.
13. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический
14. Классификация криптографических методов.

15. Традиционные (симметричные) криптосистемы.
16. Блоковые и поточные шифры.
17. Стойкость криптосистем.
18. Американский стандарт шифрования данных DES.
19. Отечественный стандарт криптографической защиты ГОСТ 28147-89.
20. Асимметричные криптосистемы.
21. Математические основы криптографии с открытым ключом.
22. Криптосистема RSA.
23. Криптосистема Эль Гамаля.
24. Криптосистемы без передачи ключей.
25. Управление ключами.
26. Методы генерации, хранения и распределения ключей.
27. Протоколы управления ключами
28. Аппаратно-программные решения защиты информации в информационных системах.
29. Аппаратно-программные средства контроля доступа.
30. iButton.
31. Смарт-карты.
32. Устройства ввода на базе USB-ключей.
33. Proximity.
34. Биометрические УВИП
35. Комбинированные устройства ввода.
36. Электронные замки.
37. Инфраструктура открытых ключей.
38. Цифровые сертификаты.
39. Электронная цифровая подпись (ЭЦП).
40. Однонаправленная хэш-функция.
41. Идентификация и аутентификация объектов сети.
42. Идентификация и подтверждение подлинности пользователей сети.
43. Математические методы обеспечения защиты от несанкционированного доступа и конфиденциальности».
44. Исторический очерк развития криптографии.
45. Криптография древнего периода.
46. Криптография арабского мира.
47. Криптография в эпоху Возрождения (XIV--XVI вв.).
48. Криптография в XVII--XVIII веках.
49. Криптография в XIX веке.
50. Криптография в XX веке.
51. О криптографии нового времени.
52. Криптография: понятия, подходы, направления исследований.
53. Базовая терминология.
54. Основные алгоритмы шифрования.
55. Цифровые подписи.
56. Криптографические хэш-функции.
57. Криптографические генераторы случайных чисел.

58. Обеспечиваемая шифром степень защиты.
59. Криптоанализ и атаки на криптосистемы.
60. Межсетевое экранирование.
61. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ.
62. Особенности межсетевого экранирования на различных уровнях модели Криптография и криптоанализ в авторизации, аутентификации и в обмене информации.
63. Основные понятия и принципы криптографии.
64. Симметричные криптосистемы.
65. Асимметричные криптосистемы.
66. Электронная цифровая подпись.
67. Управление ключами в криптографических системах защиты информации.
68. Особенности реализация криптографических методов.
69. Федеральная инфраструктура открытых ключей.
70. Направления исследований в области криптосистем.
71. Средства антивирусной защиты.
72. Классификация вирусов и средств защиты.
73. Виды антивирусных программных продуктов.
74. Характеристика наиболее популярных антивирусных пакетов.
75. Архитектура системы защиты информации (СЗИ).
76. Этапы создания СЗИ. Виды обеспечения СЗИ.
77. Принципы разработки СЗИ.
78. Информационная безопасность в глобальном информационном пространстве Интернет.
79. Безопасная интеграция в Интернет.
80. Программные и технологические решения».
81. Угрозы и риски интернет-технологий.
82. Стандартизация информационной безопасности в Интернет.
83. Программно-аппартные технологии Интернет.
84. Брандмауэры.
85. Программное обеспечение защиты информации в Интернет.
86. Основные понятия и принципы криптографии.
87. Симметричные криптосистемы.
88. Асимметричные криптосистемы.
89. Электронная цифровая подпись.
90. Управление ключами в криптографических системах защиты информации.
91. Особенности реализация криптографических методов.
92. Серверы доступа (брандмауэры) Cisco ASA5500.
93. Средства обнаружения вторжений IDS 4200.

**7.2. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Общий результат выводится как интегральная оценка, складывающая из текущего контроля - 30% и промежуточного контроля - 70%.
Текущий контроль по дисциплине включает:
- посещение занятий - 10 баллов,
- участие на практических занятиях - 10 баллов,
- выполнение домашних работ - 0 баллов.
Промежуточный контроль по дисциплине включает:
- коллоквиум - 40 баллов,
- письменная контрольная работа - 30 баллов.

**8. Учебно-методическое обеспечение дисциплины**

а) основная литература:


1. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. — Электрон.текстовые данные. — М. : Евразийский открытый институт, 2012. — 311 c. — 978-5-374-00301-7. — Режим доступа: http://www.iprbookshop.ru/10677.html
2. Галатенко, Владимир Антонович. Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности 351400 "Прикл. информ." / Галатенко, Владимир Антонович. - 4-е изд. - М. : Изд-во Интернет-Ун-та Информ. Технологий: БИНОМ. Лаб. знаний, 2016, 2008, 2006. - 205 с. - (Основы информационных технологий). - Рекомендовано УМО. - ISBN 978-5-94774-821-5 : 230-00.
Местонахождение: Университетская библиотека ONLINE, IPRbooks URL: http://biblioclub.ru/index.php?page=book&id=233063, http://www.iprbookshop.ru/52209.html
3. Мельников, Владимир Павлович. Информационная безопасность и защита информации : учеб. пособие для студентов вузов, обуч. по специальности "Информ. системы и технологии" / Мельников, Владимир Павлович, С. А. Клейменов ; под ред. С.А.Клейменова. - 5-е изд., стер. - М. : Академия, 2011, 2010. - 330,[6] с. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Допущено УМО. - ISBN 978-5-7695-7738-3 : 401-06. Местонахождение: Научная библиотека ДГУ
4. Бабаш Александр Владимирович. Информационная безопасность : лаб. практикум; учеб. пособие / Бабаш, Александр Владимирович, Е. К. Баранов. - 2-е изд., стер. - И. : Кнорус, 2016, 2011. - 306-00.
Местонахождение: Университетская библиотека ONLINE URL: http://biblioclub.ru/index.php?page=book&id=90539

б) дополнительная литература:

1. Федин Ф.О. Информационная безопасность [Электронный ресурс] : учебное пособие / Ф.О. Федин, В.П. Офицеров, Ф.Ф. Федин. — Электрон.текстовые данные. — М. : Московский городской педагогический университет, 2011. — 260 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/26486.html
2. Пятибратов Александр Петрович. Вычислительные системы, сети и телекоммуникации : [учеб. для вузов по специальности "Прикладная информатика в экономике"] / Пятибратов, Александр Петрович ; Л.П.Гудыно, А.А.Кириченко; под ред. А.П.Пятибратова. - 3-е изд., перераб. и доп. - М. : Финансы и статистика, 2005, 2003. - 558,[1] с. ; 25 см. - Библиогр.: с. 539-541. - Предм. указ.: с. 553-559. - Рекомендовано МО РФ. - ISBN 5-279-02779-0 : 257-40. Местонахождение: Научная библиотека ДГУ
3. Филин Сергей Александрович. Информационная безопасность : учеб. пособие / Филин, Сергей Александрович. - М. : Альфа-Пресс, 2006. - 411 с. - ISBN 5-94280-163-0 : 129-03. Местонахождение: Научная библиотека ДГУ
4. Расторгуев, Сергей Павлович. Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" и "Информ. безопасность телеком. систем" / Расторгуев, Сергей Павлович. - М. : Академия, 2007. - 186,[1] с. - (Высшее профессиональное образование. Информационная безопасность). - Допущено УМО. - ISBN 978-5-7695-3098-2 : 150-70. Местонахождение: Научная библиотека ДГУ

## 9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

http://www.elib.dgu.ru/
http://www.iprbookshop.ru/
http://intuit.ru/

## 10. Методические указания по освоению дисциплины

Для понимания материала и качественного его усвоения рекомендуется следующая последовательность действий:

1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст предыдущей лекции – 10-15 минут.

2. В течение недели выбрать время – 1 час для работы с литературой по программированию и анализу алгоритмов.

3. При подготовке к лабораторным занятиям, необходимо сначала прочитать основные понятия, изучить алгоритмы по теме домашнего задания. При написании программы нужно сначала понять, что требуется, какой теоретический материал нужно использовать, наметить план решения задачи. Алгоритм решения задачи – это не программа ее решения, а способ дать человеку (а не машине) представление о структуре алгоритма, о смысле его

шагов и их логической взаимосвязи. Поэтому шаги алгоритма должны описываться в терминах тех объектов и отношений между ними, о которых идет речь в условии задачи (это, конечно, не исключает использования математической и другой условной символики). Структура алгоритма станет более ясной, если ее описывать в наглядной и достаточно формализованной (напоминающей конструкции языка программирования) форме. Поэтому требуемой формой описания алгоритма в данном лабораторном практикуме является либо графическое представление алгоритма на языке блок-схем, либо на специальном языке описания алгоритмов, например школьном алгоритмическом языке.

4. Основная часть теоретического материала курса дается в ходе лекционных занятий, хотя часть материала может изучаться на лабораторных занятиях, либо самостоятельно по учебной литературе.

## 11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При осуществлении образовательного процесса по дисциплине «Информационная безопасность и защита информации» рекомендуется использовать следующие информационные технологии.

Во-первых, должны проводиться занятия с компьютерным тестированием, что приучит студентов хорошо ориентироваться с работой на компьютере для выполнения заданий.

Во-вторых, демонстрационный материал также будет показан с помощью мультимедийных устройств и интерактивной доски.

В-третьих, компьютерные классы с набором лицензионного базового программного обеспечения для проведения занятий.

## 12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

При освоении дисциплины для выполнения лабораторных работ необходимы классы персональных компьютеров с приложениями программирования на языках C/C++, а также учебные аудитории для проведения лекционных занятий.