МИНИСТЕРСТВО НАУКИ и ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
*Факультет Информатики и Информационных Технологий*

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## Программно-аппаратные средства защиты информации

Кафедра Информационных технологий и БКС

**Образовательная программа**

10.03.01 Информационная безопасность

**Профиль подготовки:**
Безопасность компьютерных систем

**Уровень высшего образования:**
бакалавриат

**Форма обучения**
Очная, очно-заочная

**Статус дисциплины**:
входит в обязательную часть ОПОП

Махачкала, 2021

Рабочая программа дисциплины «Программно-аппаратные средства защиты информации» составлена в 2021г в соответствии с требованиями ФГОС ВО - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность» от 17 ноября 2020 г. N 1427

Составитель: Ахмедова З.Х, доцент каф. ИТиБКС

Рабочая программа одобрена на заседании кафедры «Информационных технологии безопасности компьютерных систем».

Протокол № _11__ от __28.06____ 2021г

Зав кафедрой ИТиБКС _____ Ахмедова З.Х.

Одобрена на заседании Методической комиссии факультета Информатики и информационных технологий от _29.06__ 2021г протокол № 11

Председатель _____ Бакмаев А.Ш.

Рабочая программа согласована с учебно-методическим управлением

«____» _____2021г

Начальник УМУ _____ Гасангаджиева А.Г.

**Аннотация рабочей программы дисциплины.**

Дисциплина «Программно-аппаратные средства защиты информации» входит в обязательную часть образовательной программы ОПОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность.

Содержание дисциплины охватывает вопросы области установки, настройки и обслуживании программных, программно-аппаратных средств защиты информации.

Дисциплина реализуется на факультете _ИиИТ_ кафедрой ____ИТиБКС____.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональные ОПК-1, ОПК-12, профессиональные ПК-2, ПК-8.

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

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме коллоквиум, устный опрос и промежуточный контроль в форме экзамена.

Объем дисциплины 4 зачетные единицы, в том числе в академических часах по видам учебных занятий

Объем дисциплины в очной форме

| Семестр | Всего | Учебные занятия | | | | | | | Форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|
| | | в том числе | | | | | | | |
| | | Контактная работа обучающихся с преподавателем | | | | | | СРС, в том числе экзамен | |
| | | Всего | из них | | | | | | |
| | | | Лекции | Лабораторные занятия | Практические занятия | | консультации | | |
| 7 | 144 | 86 | 34 | 34 | 18 | | | 58 | экзамен |

Объем дисциплины в очно-заочной форме

| Семестр | Всего | Учебные занятия | | | | | Форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|
| | | в том числе | | | | | |
| | | Контактная работа обучающихся с преподавателем | | | | СРС, в том числе экзамен | |
| | | Всего | из них | | | | |
| | | | Лекции | Лабораторные занятия | Практические занятия | | |
| 9 | 144 | 68 | 36 | 16 | 16 | 76 | экзамен |

**1.Цели освоения дисциплины.**

Целью дисциплины «Программно-аппаратные средства защиты информации» является формирование компетенций у обучающихся в области установки, настройки и обслуживании программных, программно-аппаратных средств защиты информации.

Изучение дисциплины "Программно-аппаратные средства защиты информации " должно способствовать воспитанию у них профессиональной компетентности и профессионального кругозора, умению ориентироваться в продуктах и тенденциях развития средств защиты информационных технологий.

Задачи изучения дисциплины - дать знания по вопросам:

– угроз информационной безопасности в автоматизированных системах обработки данных;

– принципов разделения доступа и защиты программ и данных от НСД;

– использования программно-аппаратных средств защиты информации;

– проектирования систем защиты информации в АСОД.

**2.Место дисциплины в структуре ОПОП бакалавриата.**

Дисциплина Б1.О.04.02 входит в вариативную часть образовательной программы бакалавриата направлению подготовки 10.03.01 Информационная безопасность и является одной из дисциплин, в рамках которой изучаются методы и средства обеспечения информационной безопасности. Курс занимает важное место в профессиональной подготовке специалиста по защите информации. Он является одним из основных специализированных курсов. Знания, полученные в результате изучения предмета также необходимы для выполнения курсовых и дипломных работ.

Изучение данной дисциплины базируется на следующих дисциплинах:

1. Защита персональных данных
2. Техническая защита информации
3. Защита программ и данных

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин:

1. Методы оценки безопасности компьютерных систем
2. Знания, умения и навыки, полученные студентами в рамках данной дисциплины, пригодятся им при написании выпускной квалификационной работы, а также необходимы при прохождении производственной практики

**3.Компетенции обучающего, формируемые в результате освоения дисциплины.**

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

| Код и наименование компетенции из ОПОП | Код и наименование индикатора достижения | Планируемые результаты обучения | Процедура освоения |
|---|---|---|---|

| | | | |
|---|---|---|---|
| ОПК -1<br>Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; | ИД1.ОПК-1.1.Знать. организационно – правовую основу информационной безопасности и средства ее обеспечения | Знает основы математики, физики, вычислительной техники и программирования | Устный опрос, письменный опрос |
| | ИД2. ОПК-1.2.Уметь . использовать права и обязанности граждан государства в рамках правового пространства для обеспечения защиты информации | Умеет решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования | Устный опрос, письменный опрос |
| | ИД3.ОПК-1.3. Владеть навыками оперативного отслеживания нарушений прав пользователей телекоммуникационной системы и анализа информационных процессов в этих системах, способами моделирования информационных процессов в телекоммуникациях | Имеет навыки теоретического и экспериментального исследования объектов профессиональной деятельности | Устный опрос, письменный опрос |
| ОПК-12<br>Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соо*тветст*вующих проектных решений; | ИД 1 ОПК-12.1. Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта | Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта | Устный опрос, письменный опрос |
| | ИД 2 ОПК-12.2. Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации | Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации | Устный опрос, письменный опрос |
| | ИД 3 ОПК-12.3. Владеет навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных | Владеет навыками по разработке основных показателей технико-экономического обоснования | Устный опрос, письменный опрос |

| | | | |
|---|---|---|---|
| | решений | соответствующих проектных решений | |
| ПК-2 Проведение работ по установке и техническому обслуживанию защищенных технических средств обработки информации | ПК 2.1. Порядок аттестации объектов информатизации на соответствие требованиям безопасности информации; | Знает: Технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении; | Устный опрос, письменный опрос |
| | ПК 2.2. Проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией | Умеет: проводить контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок | Устный опрос, письменный опрос |
| | ПК 2.3. Способом проведения специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации; | Владеет: Проведением контроля защищенности акустической речевой информации от утечки по техническим каналам | Устный опрос, письменный опрос |
| ПК-8 Администрирование средств защиты информации в компьютерных системах и сетях | ПК-8.1. Теоретико-числовые методы и алгоритмы, применяемые в средствах защиты информации | Знает: основы теории информации | Устный опрос, письменный опрос |
| | ПК-8.2. Решать задачи сравнений по простому и составному модулям | Умеет: решать типовые задачи и формулировать прикладные задачи в терминах теории информации | Устный опрос, письменный опрос |
| | ПК-8.3. Методами решения задач разложения больших целых чисел на множители. | Владеет: основными методами исследования, использующими теории информации | Устный опрос, письменный опрос |

**4. Объем, структура и содержание дисциплины.**

**4.1.** Объем дисциплины составляет 4 зачетных единиц,

144 академических часа.

**4.2. Структура дисциплины.**

**4.2.1. Объем дисциплины в очной форме.**

| № п/п | Названия разделов | Семестр | Неделя | Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах) | | Самостоятельная | Формы текущего контроля успеваемости ( |
|---|---|---|---|---|---|---|---|

| | | | | Лекции | Практические | Лабораторные | Контроль самост работы | | по неделям семестра) Форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | | | | | | | | |
| 1 | Предмет и задачи программно-аппаратной защиты информации | 7 | 1-2 | 4 | 2 | 4 | | 2 | устный опрос |
| 2 | Программно-аппаратные средства защиты информации | 7 | 3-4 | 4 | 2 | 4 | | 2 | устный опрос |
| 3 | Контроль доступа к файлам | 7 | 5-6 | 4 | 2 | 4 | | 1 | устный опрос |
| | Итого за модуль | | | 12 | 6 | 12 | | 6 | |
| 4 | Электронная цифровая подпись (ЭЦП) | 7 | 6-7 | 4 | 2 | 4 | | 2 | устный опрос |
| 5 | Программно-аппаратные средства шифрования | 7 | 8-9 | 4 | 2 | 4 | | 1 | устный опрос |
| 6 | Методы и средства ограничения доступа | 7 | 10-11 | 4 | 2 | 4 | | 1 | устный опрос |
| | Итого за модуль | | | 12 | 6 | 12 | | 6 | |
| 7 | Защита программ | 7 | 12-13 | 2 | 2 | 2 | | 10 | устный опрос |
| 8 | Защита от разрушающих программных воздействий (РПВ) | 7 | 14-15 | 4 | 2 | 4 | | 10 | устный опрос |
| 9 | Средства предотвращения утечки информации по техническим | 7 | 16-17 | 4 | 2 | 4 | | | устный и письменный опросы |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | каналам | | | | | | | | |
| | Итого за модуль: | | | 10 | 6 | 10 | | 10 | |
| | | | | | | | | **36** | **экзамен** |
| | **Всего часов** | **144** | | **34** | **18** | **34** | | **58** | |

**4.2.2 Объем дисциплины в очно-заочной форме.**

| № п/п | Названия разделов | Семестр | Неделя | Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах) | | | | | Формы текущего контроля успеваемости ( по неделям семестра) Форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Лекции | Практические | Лабораторные | Контроль самост работы | Самостоятельная работа | |
| 1 | 2 | | | | | | | | |
| 1 | Предмет и задачи программно-аппаратной защиты информации | 9 | 1-2 | 4 | 2 | 1 | | 2 | устный опрос |
| 2 | Программно-аппаратные средства защиты информации | 9 | 3-4 | 4 | 2 | 4 | | 2 | устный опрос |
| 3 | Контроль доступа к файлам | 9 | 5-6 | 4 | 2 | 1 | | 1 | устный опрос |
| | Итого за модуль | | | 12 | 6 | 6 | | 12 | |
| 4 | Электронная цифровая подпись (ЭЦП) | 9 | 6-7 | 4 | 2 | 2 | | 2 | устный опрос |
| 5 | Программно-аппаратные средства шифрования | 9 | 8-9 | 4 | 2 | 1 | | 1 | устный опрос |
| 6 | Методы и средства ограничения доступа | 9 | 10-11 | 4 | 2 | 1 | | 1 | устный опрос |
| | Итого за модуль | | | 12 | 6 | 4 | | 14 | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 7 | Защита программ | 9 | 12-13 | 4 | 2 | 2 | | 10 | устный опрос |
| 8 | Защита от разрушающих программных воздействий (РПВ) | 9 | 14-15 | 4 | 1 | 2 | | 10 | устный опрос |
| 9 | Средства предотвращения утечки информации по техническим каналам | 9 | 16-17 | 4 | 1 | 2 | | | устный и письменный опросы |
| | Итого за модуль: | | | 12 | 4 | 6 | | 14 | |
| | | | | | | | | **36** | **экзамен** |
| | **Всего часов** | **144** | | **36** | **16** | **16** | | **76** | |

## 4.3. Содержание дисциплины, структурированное по темам (разделам).

### 4.3.1. Содержание лекционных занятий по дисциплине

Тема 1. Общие положения теории информационной безопасности. Ключевые понятия программно-аппаратных средств защиты информации и безопасных информационных технологий. Определение места программно-аппаратных средств защиты информации в общей проблеме информационной безопасности.

Тема 2. Информационные риски и статистика угроз для информации. Понятие безопасности информации и комплекс угроз в отношении оборудования пользователя и вычислительной сети. Несанкционированный доступ (НСД). Политика безопасности организации и определение субъекта, потенциально совершающего несанкционированные действия. Статьи уголовного кодекса, предусматривающие ответственность за компьютерные преступления.

Тема 3. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Сертификация средств защиты информации; Задачи и технология сертификации программноаппаратных средств на соответствие требованиям информационной безопасности; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства защиты информации в сетях передачи данных.

Тема 4. Задачи и методологические основы использования аппаратных средств защиты информации в компьютерах. Технические требования стандартов к программно-аппаратным средствам защиты информации. Международный стандарт критериев оценки формационных технологий и ГОСТ Р ИСО/МЭК 15408.

Тема 5. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Концепция диспетчера доступа. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите. Их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем.

Тема 6. Основные компоненты подсистемы защиты LINUX. Файловая система – как основа подсистемы защиты. Права доступа к элементам файловой системы. Управление процессами. Создание и удаление бюджетов пользователей. Основные проблемы с безопасностью и возможные решения в UNIX-подобных системах. Основные компоненты подсистемы защиты Windows XP, Windows 7. Политика безопасности. Понятие домена. Особенности установления доверительных отношений. Создание и удаление бюджетов пользователей.

Тема 7. Контроль целостности информации. Имитозащита информации. Криптографические методы контроля целостности. Защита информации на машинных носителях. Защита остатков информации

Тема 8. Проблема обеспечения технологической безопасности программного обеспечения. Понятие о вредоносных программах. Классификация вредоносных программ по основным свойствам и признакам. Классификация программ по степени опасности для защищаемой информации и компьютерной системы. Алгоритмические и программные закладки, мотивы злоумышленных действий. Распространение компьютерных вирусов. Спам (несанкционированные электронные письма). Классификация компьютерных вирусов. Деструктивные функции вредоносных программ. Механизмы вирусного заражения. Способы выявления деструктивной активности программ. Понятие о сигнатуре вредоносного программного кода.

Тема 9. Принцип антивирусного сканирования. Антивирусные сканеры, мониторы и сетевые фильтры. Качество антивирусной программы. Защита от разрушающих программных воздействий. Защита программ от изменения и контроль целостности.

**Темы лабораторных занятий.**

- Лабораторная работа 1. Администрирование политики безопасности ОС MS Windows.
- Лабораторная работа 2. Изучение программ идентификации и аутентификации и шифрования типовой операционной системы
- Лабораторная работа 3. Изучение методов защиты локальной ПЭВМ от НСД к информации, от несанкционированного копирования информации, идентификации и аутентификации субъектов в АС при помощи программно-аппаратного комплекса Secret Net 5.0 и электронного ключа "Соболь".
- Лабораторная работа 4. Изучение работы антивирусного программного комплекса
- Лабораторная работа 5. Изучение работы программно-аппаратного средства защиты информации «ЭЦП».

**Примерный перечень вопросов к экзамену.**

1. Нормативно-правовые и технические требования к программно-аппаратным средствам защиты информации.
2. Понятие несанкционированного доступа (НСД) к информации
3. Концепция защиты от НСД к информации
4. Основные каналы утечки информации в локальной ПЭВМ
5. Модель нарушителя при локальном НСД
6. Основные каналы утечки информации в рабочей станции
7. Показатели защищенности средств вычислительной техники от несанкционированного доступа
8. Модель нарушителя при удаленном НСД
9. Методы и средства защиты информации от НСД в локальных ПЭВМ
10. Методы и средства защиты информации от НСД на рабочих станциях в сети

11. Стандарты безопасности и их влияние на проектирование и разработку программно-аппаратных средств защиты информации
12. Принципы сертификации средств защиты информации
13. Основы разработки и проектирования программно-аппаратных комплексов обеспечения информационной безопасности.
14. Основные подходы к программно-аппаратной защите информации на автономной ЭВМ.
15. Основные подходы к программно-аппаратной защите информации на ЭВМ в локальной и глобальной сети.
16. Межсетевые экраны, их типы и конфигурация.
17. организация и администрирование работы различных типов межсетевых экранов.
18. Понятие вредоносной программы.
19. Механизмы статического скрытия вредоносного программного кода.
20. Механизмы скрытности вредоносных программ на этапе выполнения
21. Классификация и основные особенности различных видов вредоносных программ. Вредоносные действия компьютерных программ, приводящие к несанкционированной модификации компьютерной информации.

**5.Образовательные технологии.**

В учебном процессе помимо традиционных форм проведения занятий
используются лекции – визуализации, лекции – диалоги. Лабораторные занятия проводятся в компьютерном классе с использованием Интернет среды. При проведение практических занятий используются деловые игры с разбором конкретных ситуаций.

- Лекционные занятия
- Традиционные технологии
- Иллюстрация работы алгоритмов с использованием видео и элементов анимации в презентациях.
- Демонстрация элементов современных методов разработки программ с использованием видеопроектора
- Практические занятия
- Традиционные технологии
- Коллективное выполнение заданий с использованием видеопроектора, среды разработчика и системы контроля версий исходного кода SVN или Git
- Лабораторные занятия
- Традиционные технологии

**6.Учебно-методическое обеспечение самостоятельной работы студентов обучающихся по дисциплине «Программно-аппаратные средства защиты информации».**

*Форма контроля и критерий оценок*
В соответствии с учебным планом предусмотрен экзамен в седьмом семестре.
Формы контроля: текущий контроль, промежуточный контроль по модулю, итоговый контроль по дисциплине предполагают следующее распределение баллов.
Текущий контроль

- Выполнение 1 домашней работы 10 баллов
- Активность в системе Moodle 60 баллов

Примерное распределение времени самостоятельной работы студентов

| Вид самостоятельной работы | Примерная трудоёмкость, а.ч. | Примерная трудоёмкость, а.ч. | Формируемые компетенции |
|---|---|---|---|
| | Очная | Очно-заочная | |
| **Текущая СРС** | | | |
| работа с лекционным материалом, с учебной литературой | 10 | ***10*** | ОПК-1 |
| опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях) | 10 | 10 | ОПК-12 |
| самостоятельное изучение разделов дисциплины | 12 | 10 | ОПК-1 |
| выполнение домашних заданий, домашних контрольных работ | 10 | 10 | ПК-2 |
| подготовка к лабораторным работам, к практическим и семинарским занятиям | 2 | | ОПК-12, ПК-2 |
| подготовка к контрольным работам, коллоквиумам, зачётам | 10 | 10 | ПК-8 |
| подготовка к экзамену (экзаменам) | 36 | 36 | ОПК-1, ОПК-12, ПК-2, ПК-8 |
| **Творческая проблемно-ориентированная СРС** | | | |
| поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме | 10 | 20 | ОПК-1 |
| исследовательская работа, участие в конференциях, семинарах, олимпиадах | 10 | 14 | ОПК-12 |
| анализ данных по заданной теме, написание программ, составление моделей на основе исходных данных | 2 | 10 | ПК-2, ПК-8 |
| ИТОГО: | 102ч | 130ч | |

**Рекомендуемая литература.**

а) основная литература:


1. Долозов Н. Л., Гультяева Т. А. \\ Программные средства защиты информации: конспект лекций \\ Новосибирск: Новосибирский государственный технический университет, 2015. – 63 с. Режим доступа: http://www.iprbookshop.ru/48034.html.— ЭБС «IPRbooks»[Дата обращения 20 июня 2021]
2. Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков \\ Программно-аппаратные средства защиты информационных систем: учебное пособие \\ Тамбов: Издательство ФГБОУ ВО «ТГТУ», 2017. – 194 с. Режим доступа: http://www.iprbookshop.ru/42037.html.— ЭБС «IPRbooks»[Дата обращения 20 июня 2021]


б) дополнительная литература:


1. Свинарёв Н.А., Ланкин О.В., Данилкин А.П., Потехецкий С.П., Перетокин О.И. \\ Инструментальный контроль и защита информации: учебное пособие \\ Воронеж: Воронежский государственный университет инженерных технологий, 2013. – 192 с. Режим доступа: http://www.iprbookshop.ru/43064.html.— ЭБС «IPRbooks»[Дата обращения 20 июня 2021]


## 7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ

**УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.**

**7.1. Типовые контрольные задания или иные материалы**

**ПРИМЕРЫ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ МАТЕРИАЛОВ**

**№Текст тестовых материалов**

1. Информационная безопасность характеризует защищённость:
А) Пользователя и информационной системы
Б) Информации и поддерживающей еѐ инфраструктуры
В) Источника информации
Г) Носителя информации

2. Что из перечисленного является составляющей информационной безопасности?
А) Нарушение целостности информации
Б) Проверка прав доступа к информации
В) Доступность информации
Г) Выявление нарушителей

3. Получение требуемой информации информационной услуги пользователем за определѐнное время, это:
А) Целостность информации
Б) Конфиденциальность информации
В) Доступность информации
Г) Защищенность информации

4. Конфиденциальность информации гарантирует:
А) Доступность информации кругу лиц, для кого она предназначена
Б) Защищѐнность информации от потери
В) Защищѐнность информации от фальсификации
Г) Доступность информации только автору

9. Основной источник внутренних отказов?
А) Невозможность пользователя работать с системой в силу отсутствия соответствующей подготовки
Б) Нежелание пользователя работать с информационной системой
В) Отступление от установленных правил эксплуатации
Г) Нарушение работы систем связи, электропитания, водо-и/или теплоснабжения, кондиционирования

10. Уровни не относящиеся к уровням формирования режима информационной безопасности?
А) Законодательно-правовой
Б) Информационный
В) Административный (организационный)
Г) Программно-технический

11. На сколько классов подразделяют угрозы информационной безопасности?
А) 4
Б) 3
В) 2

Г) 5

12. Что является самым эффективным при борьбе с непреднамеренными случайными ошибками?
А) Резервирование аппаратуры
Б) Определение степени ответственности за ошибки
В) Максимальная автоматизация и строгий контроль
Г) Контроль действий пользователя

13. Средства защиты информации какого из уровней формирования режима информационной безопасности связаны непосредственно с защищаемой информацией
А) Законодательно-правовой
Б) Информационный
В) Административный (организационный)
Г) Программно-технический

20. Что из перечисленного является задачей информационной безопасности?
А) Устранение неисправностей аппаратных средств
Б) Устранение последствий стихийных бедствий
В) Защита технических и программных средств информатизации от ошибочных действий персонала
Г) Восстановление линий связи

21. Выберите правильную иерархию пространства требований в «Общих критериях»:
А) Класс –семейство –компонент –элемент
Б) Элемент –класс –семейство –компонент
В) Компонент –семейство – класс –элемент
Г) Семейство –компонент –класс –элемент

22. Сколько классов СВТ по уровню защищенности от НСД к информации определено в руководящем документе Гостехкомиссии «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»?
А) Три
Б) Семь
В) Пять
Г)Четыре

23. Комплекс предупредительных мер по обеспечению информационной безопасности организации –это:
А) Информационная политика
Б) Политика безопасности
В) Информационная безопасность
Г) Защита информации

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

Фонд оценочных средств дисциплины включает в себя контрольные вопросы, задания контрольных работ, вопросы для промежуточной аттестации. Виды самостоятельной работы обучающихся. Изучение основной и дополнительной литературы по материалам курса.

Выполнение заданий самостоятельной работы по курсу.

Таблица максимальных баллов по видам учебной деятельности

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| Семестр | Лекции | Лабора-торные занятия | Практические занятия | Само-стоя-тельная работа | Автоматизированное тести-рование | Другие виды учебной дея-тельности | Промежуточная аттестация | Итого |
| 7 | 5 | 10 | 15 | 25 | 0 | 5 | 40 | 100 |

Программа оценивания учебной деятельности студента. Семестр 7
**Лекции.** Посещаемость, опрос, активность за семестр — от 0 до 5 баллов.
**Лабораторные занятия.** Выполнение одной лабораторной работы – 10б.
**Практические занятия.** Посещаемость, опрос, активность за семестр — от 0 до 15 баллов.
**Самостоятельная работа.** Контроль выполнения заданий самостоятельной работы в течение одного семестра — от 0 до 25 баллов;
**Контрольная работа** (от 0 до 10 баллов);
**Автоматизированное тестирование.** Не предусмотрено.
**Другие виды учебной деятельности.**
Написание реферата является одной из форм обучения студентов. Данная форма обучения направлена на организацию и повышение уровня самостоятельной работы студентов. Реферат, как форма обучения студентов - это краткий обзор максимального количества доступных публикаций по заданной теме, подготовка самого реферативного обзора и презентации по нему. При проведении обзора должна проводиться и исследовательская работа, но объем ее ограничен, так как анализируется уже сделанные выводы и в связи с небольшим объемом данной формы работы. Преподавателю предоставляется сам реферат в письменной форме (электронная версия в формате Microsoft Word) и презентация к нему (электронная версия в формате PowerPoint). Сдача реферата происходит в форме защитыдоклада с использованием подготовленной презентации.
**Критерии оценки рефератов:**
**Оценки на "отлично":**
10 - тема раскрыта блестяще, презентация является целостным новым независимым дополнением высокого уровня к лекционному курсу
9 - тема раскрыта отлично, есть отдельные фрагменты, которые являются новыми независимыми смысловыми дополнениями к лекциям
8 - тема в основном раскрыта, качество материала высокое, но не является уникальным
**Оценки на "хорошо"**
7 - тема раскрыта не полностью, не хватает некоторой части. Качество материала хорошее.
6 - тема раскрыта не полностью, не хватает некоторой значимой части.
**Удовлетворительно:**
5 - раскрыта хотя бы примерно половина темы. Качество материала удовлетворительное.
4 - что-то по существу реферата сказано, но мало и фрагментарно. Качество материала на грани удовлетворительного.
**Неудовлетворительно:**
3 - понял, о чем надо рассказывать, но практически ничего не рассказал по теме реферата. Качество материала неудовлетворительное.
2 - понял название темы, ничего не рассказал либо рассказывал не о том. Материал фактически отсутствует.
1 - не понял название темы, не рассказывал. Материал фактически отсутствует и не по теме.
0 - реферат не сдавался.

**Промежуточная аттестация.** Методика оценивания знаний, обучающихся по дисциплине «Облачные технологии» в ходе промежуточной аттестации:
25-40 баллов:
Ответ студента содержит:
глубокое знание программного материала, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой;
знание концептуально-понятийного аппарата всего курса;
знание монографической литературы по курсу,
также свидетельствует о способности:
самостоятельно критически оценивать основные положения курса;
увязывать теорию с практикой.
15-24 баллов:
Ответ студента свидетельствует:
о полном знании материала по программе;
о знании рекомендованной литературы,
а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.
1-14 баллов:
Ответ студента содержит:
поверхностные знания важнейших разделов программы и содержания лекционного курса;
затруднения с использованием научно-понятийного аппарата и терминологии курса;
стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.
Студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала ставится оценка 0 баллов.
Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за один семестр по дисциплине «Облачные технологии» составляет 100 баллов.

Итоговой формой контроля знаний, умений и навыков по дисциплине является **Экзамен**. Экзамен проводится в форме тестирования. При соответствии ответа учащегося на зачете более чем 51 % критериев из этого списка выставляется оценка «удовлетворительно», 66% – 85% оценка «хорошо», 86% и выше оценка «отлично».

## 8.Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) основная литература:


1. Долозов Н. Л., Гультяева Т. А. \\ Программные средства защиты информации: конспект лекций \\ Новосибирск: Новосибирский государственный технический университет, 2015. – 63 с. Режим доступа: http://www.iprbookshop.ru/48034.html.— ЭБС «IPRbooks»[Дата обращения 20 июня 2021]
3. Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков \\ Программно-аппаратные средства защиты информационных систем: учебное пособие \\ Тамбов: Издательство ФГБОУ ВО «ТГТУ», 2017. – 194 с. Режим доступа: http://www.iprbookshop.ru/42037.html.— ЭБС «IPRbooks»[Дата обращения 20 июня 2021]


б) дополнительная литература:


2. Свинарёв Н.А., Ланкин О.В., Данилкин А.П., Потехецкий С.П., Перетокин О.И. \\ Инструментальный контроль и защита информации: учебное пособие \\ Воронеж: Воронежский государственный университет инженерных технологий, 2013. – 192 с. Режим доступа: http://www.iprbookshop.ru/43064.html.— ЭБС «IPRbooks»[Дата обращения 20 июня 2021]

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

1. eLIBRARY.Ru[Электронный ресурс]: электронная библиотека / Науч. электр. б-ка.- МОСКВА.1999. – Режим доступа: http//elibrary.ru (дата обращения 15.04.2018). – Яз. рус., англ.
2. Электронный каталог НБ ДГУ Ru [Электронный ресурс]: база данных содержит сведения о всех видах лит., поступающих в фонд НБ ДГУ / Дагестанский гос.унив. – Махачкала. – 2010. – Режим доступа: http//elib.dgu.ru. свободный (дата обращения 11.03.2018)
3. Национальный Открытый Университете «ИНТУИТ»[ Электронный ресурс]: электронно-библиотечная система, издательство «Лань» - www.intuit.ru(дата обращения 12.03.2018)

## 10. Методические указания для обучающихся по освоению дисциплины.

К современному специалисту общество предъявляет достаточно широкий перечень требований, среди которых немаловажное значение имеет наличие у выпускников определенных способностей и умения самостоятельно добывать знания из различных источников, систематизировать полученную информацию, давать оценку конкретной финансовой ситуации. Формирование такого умения происходит в течение всего периода обучения через участие студентов в практических занятиях, выполнение контрольных заданий и тестов, написание курсовых и выпускных квалификационных работ. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

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

1. Компьютерные классы с набором лицензионного базового программного обеспечения для проведения лабораторных занятий;

2. MicrosoftVisualStudio (или CodeBloc) для выполнения лабораторных заданий

3. Лекционная мультимедийная аудитория для чтения лекций с использованием мультимедийных материалов.

4. Тестовая программа Test2000 для компьютерного тестирования.

## 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 С/С++. Для проведения лекционных занятий, необходима мультимедийная аудитория с набором лицензионного базового программного обеспечения.

**Лекционные занятия**

- Видеопроектор, ноутбук, презентатор
- Подключение к сети Интернет

**Практические занятия**

- Видеопроектор, ноутбук
- Подключение к сети Интернет