Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 01.09.2023 12:26:52
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

**УТВЕРЖДЕНО**
Декан факультета
Информационных технологий
_____ / Демидов Д.Г. /
«27» апреля 2022 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## «Методы и средства защиты компьютерной информации»

Направление подготовки
**09.03.01 «Информатика и вычислительная техника»**

Образовательная программа (профиль подготовки)
**«Электронные системы управления»**

Квалификация (степень) выпускника
**Бакалавр**

Форма обучения
**Очная**

Москва 2022 г.

Программа дисциплины «Методы и средства защиты компьютерной информации» составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению **09.03.01 «Информатика и вычислительная техника»** по профилю подготовки **«Киберфизические системы»**

Программу составил:
к.ф.-м.н. _____ /Т.Т. Идиатуллов/

Программа дисциплины «Методы и средства защиты компьютерной информации» **09.03.01 «Информатика и вычислительная техника»** по профилю подготовки **«Киберфизические системы»** утверждена на заседании кафедры «СМАРТ-технологии»

«_26_» ___апреля__ 2022_ г. протокол № _8____

И.О. Зав. кафедрой _____ /Я.В. Береснева/

## 1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Методы и средства защиты компьютерной информации» следует отнести:

- формирование у студентов знаний о методах и средствах защиты компьютерной информации, о принципах преобразования информации в вид, затрудняющий или делающий невозможным несанкционированные операции с нею;

– подготовка студентов к деятельности в соответствии с квалификационной характеристикой бакалавра по направлению.

К **основным задачам**освоения дисциплины «Методы и средства защиты компьютерной информации» следует отнести:

- ознакомление с основными понятиями, относящимися к области защиты компьютерной информации в технических системах управления;

- овладение современными методами шифрования в криптографии информационных потоков технических систем управления;

- овладение программно-аппаратными комплексами защиты компьютерной информации;

- овладение основными классификационными признаками компьютерных вирусов и методами защиты от них;

- овладение стандартами и спецификациями в области информационной безопасности систем управления.

## 2. Место дисциплины в структуре ООП бакалавриата.

Дисциплина «Методы и средства защиты компьютерной информации» относится к числу профессиональных учебных дисциплин по выбору базового цикла (Б1) основной образовательной программы бакалавриата.
«Методы и средства защиты компьютерной информации» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП:

*В базовой части Блока 1:*

*-Математика;*
*- Физика;*
*-Программирование и основы алгоритмизации;*
*- Вычислительные машины, системы и сети.*

*В вариативной части Блока 1:*

*-Технические измерения и приборы;*
*-Цифровая обработка сигналов;*
*-Основы управления;*
*-Дискретная математика.*

### 3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

| **Код компетенции** | **В результате освоения образовательной программы обучающийся должен обладать** | **Перечень планируемых результатов обучения по дисциплине** |
|---|---|---|
| ОПК-1 | способностью применять естественно-научные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности | **знать:**<br>● о методах математического анализа и моделирования. Знать основную теорию об экспериментальных исследованиях в профессиональной деятельности<br>**уметь:**<br>● применять естественно-научные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности<br>**владеть:**<br>● навыками применения полученных знаний и навыками общеинженерного моделирование<br>● умениями проводить экспериментальные исследования |
| ОПК-2 | способностью использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности | **знать:**<br>● о теорию о самых современных информационных технологиях и программных средствах, методах их применения в профессиональной деятельности<br>**уметь:**<br>● использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности<br>**владеть:**<br>● навыками применения самых современных информационных технологий и программных средств в решении поставленной задачи |

| | | |
|---|---|---|
| ОПК-9 | Способностью осваивать методики использования программных средств для решения практических задач | **знать:**<br>● о методиках использования программных средств для решения практических задач<br>**уметь:**<br>● на практике применять освоенные методики использования программных средств для решения практических задач<br><br>**владеть:**<br>● навыками освоения различных методик, с помощью которых можно использовать программные средства |
| ПК-2 | Способностью разрабатывать требования и проектировать программное обеспечение | **знать:**<br>● основные принципы написания программного кода, алгоритма<br>**уметь:**<br>● оперировать командами языка программирования и писать код, разрабатывать алгоритм, необходимы для решения поставленной задачи<br>**владеть:**<br>● навыками решения поставленных задач, знаниями об используемом языке программирования |

## 4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет **3** зачетные единицы, т.е. **108** академических часа (из них 72 часа – самостоятельная работа студентов).

Разделы дисциплины «Методы и средства защиты компьютерной информации» изучаются на пятом семестре третьего курса.

**На пятом** семестре выделяется **3** зачетных единицы, т.е. **108** академических часа (из них**72** часа – самостоятельная работа студентов), лабораторные работы – 1 зачетная единица, т.е.4 часа в две недели.

**Седьмой семестр:** лабораторные работы – 36 часов в семестр, форма контроля – зачет.

Структура и содержание дисциплины «Методы и средства защиты компьютерной информации» по срокам и видам работы отражены в приложении 1.

### Содержание разделов дисциплины

**Семестр 5**

**Введение**

Основные понятия, положения и определения. Предмет и объект защиты. Понятие угрозы безопасности. Классификация угроз. Классификация злоумышленников. Основные методы реализации угроз информационной безопасности. Причины, виды и каналы утечки информации.

**Правовые и организационные методы защиты компьютерной информации.**

Правовое регулирование в области безопасности информации. Государственная политика РФ в области безопасности информационных технологий. Законодательная база в области информационных технологий. Структура государственных органов, обеспечивающих безопасность информационных технологий. Общая характеристика организационных методов защиты.

**Стандарты и спецификации в области информационной безопасности.**

Общие критерии безопасности. Подготовка и целевая направленность общих критериев. Организация общих критериев. Возможности и применимость, концепции общих критериев. Действующие стандарты и рекомендации в области информационной безопасности. Критерии оценки надежных компьютерных систем («Оранжевая книга» Министерства обороны США). Гармонизированные критерии европейских стран. Руководящие документы по защите от несанкционированного доступа Гостехкомиссии при президенте РФ. Особенности информационной безопасности компьютерных сетей. Рекомендации X.800.

**Административный уровень информационной безопасности в информационно-вычислительной системе.**

Понятие политики безопасности**.** Анализ риска.Угрозы/видимость. Уязвимость/последствия. Учет информационных ценностей. Модели основных типов политик безопасности. Типы политик безопасности. Модель матрицы доступов Харрисон-Руззо-Ульмана. Модель распространения прав доступа Take-Grant. Модель системы безопасности Белла-Лападула. Модель Low-Water-Mark. Модель ролевого разграничения доступа.

**Криптографическая защита информации.**

Основные определения криптологии. Классификация методов криптографического закрытия информации. Основы теории К.Шеннона. Основные криптографические модели. Алгоритмы шифрования. Симметричные методы шифрования. Асимметричные методы шифрования. Сравнение криптографических методов. Методы кодирования. Другие методы.

**Защита компьютерной информации в локальных ЭВМ и информационно-вычислительных сетях.**

Модели безопасности основных операционных систем. Механизмы защиты операционных систем. Система безопасности WindowsNT. Защита в операционной системе NovellNetware.

**Системы защиты программного обеспечения.**

Классификация систем защиты программного обеспечения. Достоинства и недостатки основных систем защиты. Упаковщики/шифраторы. Системы защиты от несанкционированного копирования. Системы защиты от несанкционированного доступа. Показатели эффективности систем защиты.

**Защита информации в корпоративных сетях.**

Основы и цель политики безопасности в компьютерных сетях. Управление доступом. Идентификация и установление подлинности. Проверка полномочий субъектов на доступ к ресурсам. Регистрация обращений к защищаемым ресурсам. Реагирование на несанкционированные действия. Многоуровневая защита корпоративных сетей. Аутентификация. Анализ возможностей маршрутизации и прокси-серверов. Типы межсетевых экранов.

**Защита от информационных инфекций. Вирусология.**

Классификация компьютерных вирусов. Профилактика и лечение информационных инфекций. Программы обнаружения и защиты от вирусов.

## 5. Образовательные технологии.

Методика преподавания дисциплины «Методы и средства защиты компьютерной информации» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятийв сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- подготовка к лекциям и зачету в форме самостоятельной работы студентов;
- подготовка к выполнению лабораторных работ, выполнение в виде Отчетов и их защита;
– подготовка, представление и обсуждение презентаций;
– организация, проведение текущего контроля знаний;
- обсуждение и защита рефератов по дисциплине.

.

## 6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

**В седьмом семестре**

- в процессе обучения предусмотрены доклады студентов;
- индивидуальный опрос;
- в процессе обучения предусмотрен реферат с последующим обсуждением и защитой;
- подготовка к выполнению лабораторных работ и их защита;
- зачет по материалам седьмого семестра.

Оценочные средства текущего контроля успеваемости включают контрольные вопросы и задания для контроля освоения обучающимися разделов дисциплины.

Примерные темы рефератов, перечень лабораторных работ, темы докладов, контрольных вопросов для проведения текущего контроля, вопросы к зачету приведены в приложении.

### 6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

#### 6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

| Код компетенции | В результате освоения образовательной программы обучающийся должен обладать |
|---|---|
| ОПК-1 | Способностью применять естественно-научные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности |
| ОПК-2 | способностью использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности |
| ОПК-9 | Способностью осваивать методики использования программных средств для решения практических задач |
| ПК-2 | Способностью разрабатывать требования и проектировать программное обеспечение |

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

#### 6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю).

| **ОПК-1** - Способностью применять естественно-научные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности | | | | |
|---|---|---|---|---|
| **Показатель** | **Критерии оценивания** | | | |
| | **2** | **3** | **4** | **5** |
| **знать:**<br>● о методах математического анализа и моделирования. Знать основную теорию об экспериментальных исследованиях в профессиональной деятельности | Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. | Обучающийся демонстрирует неполное соответствие следующих знаний: физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам.Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся | Обучающийся демонстрирует частичное соответствие следующих знаний: физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам,но допускаются незначительные ошибки, неточности, затруднения при | Обучающийся демонстрирует полное соответствие следующих знаний:физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналамфизические |

| | | | | |
|---|---|---|---|---|
| | | испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации. | аналитических операциях. | процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналамкономерности свободно оперирует приобретенными знаниями. |
| **уметь:**<br>● применять естественно-научные и общеинженерные знания, методы математического анализа и | Обучающийся не умеет или в недостаточной степени умеет рационально выбирать различныефизические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно- | Обучающийся демонстрирует неполное соответствие следующих умений: рационально выбирать различные физические процессы в компьютерных системах и сетях, | Обучающийся демонстрирует частичное соответствие следующих умений: рационально выбирать различные физические процессы в компьютерных | Обучающийся демонстрирует полное соответствие следующих умений: рационально выбирать различные. |

| | | | | |
|---|---|---|---|---|
| моделирования, теоретического и экспериментального исследования в профессиональной деятельности | телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. | способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам, нодопускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при ихпереносе на новые ситуации. | системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации. | физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналамСвободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности. |
| **владеть:**<br>● навыками применения | Обучающийся не владеет или в недостаточной степени владеет навыкамивыбирать различныефизические процессы в | Обучающийся владеет навыкамивыбирать различныефизические процессы в | Обучающийся частично владеет навыками выбирать различныефизически | Обучающийся в полном объеме владеет навыками н выбирать |

| | | | | |
|---|---|---|---|---|
| полученных знаний и навыками общеинженерного моделирования<br>• умениями проводить экспериментальные исследования | компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. | компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам.<br>.Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях. | е процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам..Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации. | различныефизические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам, свободно применяет полученные навыки в ситуациях повышенной сложности. |
| ОПК-2 – Способностью использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности | | | | |
| **знать:** | Обучающийся демонстрирует | Обучающийся демонстрирует | Обучающийся демонстрирует частичное соответствие следующих знаний: | Обучающийся демонстрирует |

| | | | | |
|---|---|---|---|---|
| ● о теорию о самых современных информационных технологиях и программных средствах, методах их применения в профессиональной деятельности | полное отсутствие или недостаточное соответствие следующих знаний: физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. | неполное соответствие следующих знаний: физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам.Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые | физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам,но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях. | полное соответствие следующих знаний:физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналамфизические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в |

| | | | | |
|---|---|---|---|---|
| | | ситуации. | | информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналамкономерности свободно оперирует приобретенными знаниями. |
| **уметь:**<br>● использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности | Обучающийся не умеет или в недостаточной степени умеет рационально выбирать различныефизические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по | Обучающийся демонстрирует неполное соответствие следующих умений: рационально выбирать различные физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникацион | Обучающийся демонстрирует частичное соответствие следующих умений: рационально выбирать различные физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно- | Обучающийся демонстрирует полное соответствие следующих умений: рационально выбирать различные. физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналамСвободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности. |

| | | | | |
|---|---|---|---|---|
| | техническим каналам. | ных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам, нодопускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при ихпереносе на новые ситуации. | телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации. | |
| **владеть:**<br>● навыками применения самых современных информационных технологий и программных средств в решении поставленной задачи | Обучающийся не владеет или в недостаточной степени владеет навыкамивыбирать различныефизические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных | Обучающийся владеет навыкамивыбирать различныефизические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в | Обучающийся частично владеет навыками выбирать различныефизические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, | Обучающийся в полном объеме владеет навыками н выбирать различныефизические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных |

| | | | | |
|---|---|---|---|---|
| | системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. | информационно-телекоммуникационн ых системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. .Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях. | обрабатываемой в информационно-телекоммуникацион ных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам..Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации. | системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам, свободно применяет полученные навыки в ситуациях повышенной сложности. |
| **ОПК-9** - способностью осваивать методики использования программных средств для решения практических задач | | | | |
| **знать:**<br>о методиках использования программных средств для решения практических задач | Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: физические процессы в компьютерных системах и сетях, | Обучающийся демонстрирует неполное соответствие следующих знаний: физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и | Обучающийся демонстрирует частичное соответствие следующих знаний: физические процессы в компьютерных системах и сетях, способствующие | Обучающийся демонстрирует полное соответствие следующих знаний:физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты |

| | | | | |
|---|---|---|---|---|
| | способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. | средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам.Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации. | утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам,но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях. | информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналамфизические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналамкономерности свободно оперирует приобретенными знаниями. |
| **уметь:**<br>● на практике применять освоенные методики использования программных средств для решения | Обучающийся не умеет или в недостаточной степени умеет рационально | Обучающийся демонстрирует неполное соответствие следующих умений: рационально выбирать | Обучающийся демонстрирует частичное соответствие следующих умений: | Обучающийся демонстрирует полное соответствие следующих умений: рационально выбирать различные. |

| | | | | |
|---|---|---|---|---|
| практических задач | выбирать различныефизически е процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникацион ных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. | различные физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационны х системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам, нодопускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при ихпереносе на новые ситуации. | рационально выбирать различные физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникацион ных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации. | физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналамСвободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности. |
| **владеть:** | Обучающийся не | Обучающийся владеет | Обучающийся | Обучающийся в полном |

| | | | | |
|---|---|---|---|---|
| • навыками освоения различных методик, с помощью которых можно использовать программные средства | владеет или в недостаточной степени владеет навыкамивыбирать различныефизические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. | навыкамивыбирать различныефизические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. .Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях. | частично владеет навыками выбирать различныефизические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам..Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации. | объеме владеет навыками н выбирать различныефизические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам, свободно применяет полученные навыки в ситуациях повышенной сложности. |
| **ПК-2** - способностью разрабатывать требования и проектировать программное обеспечение | | | | |

| | | | | |
|---|---|---|---|---|
| **знать:**<br>● основные принципы написания программного кода, алгоритма | Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. | Обучающийся демонстрирует неполное соответствие следующих знаний: физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам.Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации. | Обучающийся демонстрирует частичное соответствие следующих знаний: физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам,но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях. | Обучающийся демонстрирует полное соответствие следующих знаний:физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам закономерности |

| | | | | |
|---|---|---|---|---|
| | | | | свободно оперирует приобретенными знаниями. |
| **уметь:**<br>● оперировать командами языка программирования и писать код, разрабатывать алгоритм, необходимы для решения поставленной задачи | Обучающийся не умеет или в недостаточной степени умеет рационально выбирать различные физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. | Обучающийся демонстрирует неполное соответствие следующих умений: рационально выбирать различные физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам, не допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает | Обучающийся демонстрирует частичное соответствие следующих умений: рационально выбирать различные физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. Умения освоены, но допускаются незначительные ошибки, неточности, | Обучающийся демонстрирует полное соответствие следующих умений: рационально выбирать различные. физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности. |

| | | | | |
|---|---|---|---|---|
| | | значительные затруднения при оперировании умениями при их переносе на новые ситуации. | затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации. | |
| **владеть:**<br>● навыками решения поставленных задач, знаниями об используемом языке программирования | Обучающийся не владеет или в недостаточной степени владеет навыками выбирать различные физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам. | Обучающийся владеет навыками выбирать различные физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам.<br>.Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях. | Обучающийся частично владеет навыками выбирать различные физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам..Навыки освоены, но допускаются незначительные | Обучающийся в полном объеме владеет навыками н выбирать различные физические процессы в компьютерных системах и сетях, способствующие утечке защищаемой информации, методы и средства защиты информации, обрабатываемой в информационно-телекоммуникационных системах, методы и средства контроля эффективности защиты информации от утечки по техническим каналам, свободно применяет полученные навыки в ситуациях повышенной сложности. |

| | | | | |
|---|---|---|---|---|
| | | | ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации. | |

**Шкалы оценивания результатов промежуточной аттестации и их описание:**
**Форма промежуточной аттестации: зачет.**

Промежуточная аттестация обучающихся в форме зачёта проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «зачтено» или «не зачтено».

*К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине «Методы и средства защиты компьютерной информации»*

| **Шкала оценивания** | **Описание** |
|---|---|
| Зачтено | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. |
| Не зачтено | Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации. |

Фонды оценочных средствпредставлены в приложении 2 к рабочей программе.

## 7. Учебно-методическое и информационное обеспечение дисциплины.

**а) основная литература:**

1. Щербаков А. Современная компьютерная безопасность. Теоретические основы. Практические аспекты: учебное пособие:– Книжный мир, 2009 г. – 352 с. (http://www.knigafund.ru/books/181313).

2. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие:– Директ-Медиа, 2015 г. – 253 с. http:/www.knigafund.ru/books/181420

**б) дополнительная литература:**

1. Скрипник Д. А. Общие вопросы технической защиты информации:–

Национальный Открытый Университет «ИНТУИТ», 2016 г.– 425 с.

**в) вспомогательная литература**

1. Карпов В.А. Методы и средства защиты компьютерной информации. Курс лекций. М., МИРЭА. 2006.

2. Ярочкин В.И. Информационная безопасность. Учебник для вузов. Академический проект. 2006.

3. Баричев С.Г. Основы современной криптографии /С.Г.Баричев, В.В.Гончаров, Р.Е.Серов. – М.: Горячая линия – Телеком, 2001.- 121с.

4. Безруков Н.Н. Компьютерные вирусы. М., Наука, 1991. 5. Горячев Г.А. Методы и средства защиты компьютерной информации. Методические указания к лабораторному практикуму. СПб., ЛЭТИ. 2006.

**г) программное обеспечение и интернет-ресурсы:**

Интернет-ресурсы включают учебно-методические материалы в электронном виде, представленные на сайте http://lib.mami.ru/ebooks/ в разделе «Библиотека».

**Полезные учебно-методические и информационные материалы представлены на сайтах:**

1. Автоматизация производственных процессов, Волчкевич Л.И.: Учебн. пособие. – 2-е изд., - М: Машиностроение, 2007. – 380 с. https://e.lanbook.com/reader/book/726/#7

2. Автоматизация и современные технологии. (http://www.mashin.ru/jurnal/content.php?id=2) 3. Автоматизация в промышленности. (http://www.avtprom.ru/)

## 8. Материально-техническое обеспечение дисциплины.

Аудитория кафедры «Автоматика и управление» АВ2602 – «Диагностика и надежность»
Компьютерные классы «Автоматика и управление» ауд. АВ2614, АВ2618, АВ2507

Оборудование и аппаратура:
- проектор с компьютером и подборкой материалов для лекций и практическихзанятий.

## 9. Методические рекомендации для самостоятельной работы студентов

Самостоятельная работа является одним из видов учебных занятий. Цель самостоятельной работы – практическое усвоение студентами вопросов информационной безопасности современных информационных технологий в процессе жизненного цикла изделия, рассматриваемых в процессе изучения дисциплины.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия.

**Задачи самостоятельной работы студента**:

- развитие навыков самостоятельной учебной работы;
- освоение содержания дисциплины;
- углубление содержания и осознание основных понятий дисциплины;
- использование материала, собранного и полученного в ходе самостоятельных занятий для эффективной подготовки к зачету.

**Виды внеаудиторной самостоятельной работы:**

- самостоятельное изучение отдельных тем дисциплины;
- подготовка к лекционным занятиям;
- подготовка к лабораторным работам;
- подготовка к семинарам и практическим занятиям;
- выполнение домашних заданий по закреплению тем;
- составление и оформление докладов по отдельным темам программы;
- подготовка и защита реферата.

Для выполнения любого вида самостоятельной работы необходимо пройти следующие этапы:

- определение цели самостоятельной работы;
- конкретизация познавательной задачи;
- самооценка готовности к самостоятельной работе;
- выбор адекватного способа действия, ведущего к решению задачи;
- планирование работы (самостоятельной или с помощью преподавателя) над заданием;
- осуществление в процессе выполнения самостоятельной работы самоконтроля (промежуточного и конечного) результатов работы и корректировка выполнения работы;
- рефлексия;
- презентация работы.

**Вопросы, выносимые на самостоятельную работу(ОПК-3;ОПК-9)**

**Семестр 7**

-Основные понятия, положения и определения защиты информации в информационно-вычислительных системах.
-Предмет и объект защиты. Понятие угрозы безопасности.
-Классификация угроз. Классификация злоумышленников.
- Основные методы реализации угроз информационной безопасности.
-Причины, виды и каналы утечки информации.
-Правовые и организационные методы защиты компьютерной информации.
-Правовое регулирование в области безопасности информации.
-Государственная политика РФ в области безопасности информационных технологий.
-Законодательная база в области информационных технологий.
- Структура государственных органов, обеспечивающих безопасность информационных технологий.
- Общая характеристика организационных методов защиты.
-Стандарты и спецификации в области информационной безопасности.
-Общие критерии безопасности. Подготовка и целевая направленность общих критериев.
-Организация общих критериев. Возможности и применимость, концепции общих критериев.
- Действующие стандарты и рекомендации в области информационной безопасности.

-Критерии оценки надежных компьютерных систем («Оранжевая книга» Министерства обороны США).
- Гармонизированные критерии европейских стран.
- Руководящие документы по защите от несанкционированного доступа Гостехкомиссии при президенте РФ.
- Особенности информационной безопасности компьютерных сетей. Рекомендации X.800.
-Административный уровень информационной безопасности в информационно-вычислительной системе.
-Понятие политики безопасности**.** Анализ риска.Угрозы/видимость. Уязвимость/последствия.
-Учет информационных ценностей. Модели основных типов политик безопасности.
-Типы политик безопасности. Модель матрицы доступов Харрисон-Руззо-Ульмана.
-Модель распространения прав доступа Take-Grant.
-Модель системы безопасности Белла-Лападула.
- Модель Low-Water-Mark.
- Модель ролевого разграничения доступа.
-Криптографическая защита информации**.**Основные определения криптологии.
- Классификация методов криптографического закрытия информации.
-Основы теории К. Шеннона.
- Основные криптографические модели. Алгоритмы шифрования.
-Симметричные методы шифрования.
-Асимметричные методы шифрования.
-Сравнение криптографических методов.
- Методы кодирования. Другие методы.
-Защита компьютерной информации в локальных ЭВМ и информационно-вычислительных сетях.
-Модели безопасности основных операционных систем. Механизмы защиты операционных систем.
- Система безопасности WindowsNT.
- Защита в операционной системе NovellNetware.
-Системы защиты программного обеспечения.Классификация систем защиты программного обеспечения.
-Достоинства и недостатки основных систем защиты. Упаковщики/шифраторы.
-Системы защиты от несанкционированного копирования.
- Системы защиты от несанкционированного доступа. Показатели эффективности систем защиты.
-Защита информации в корпоративных сетях.Основы и цель политики безопасности в компьютерных сетях.
- Управление доступом. Идентификация и установление подлинности.
-Проверка полномочий субъектов на доступ к ресурсам. Регистрация обращений к защищаемым ресурсам.
- Реагирование на несанкционированные действия.
- Многоуровневая защита корпоративных сетей. Аутентификация.
- Анализ возможностей маршрутизации и прокси-серверов.
-Типы межсетевых экранов.
-Защита от информационных инфекций. Вирусология.
-Классификация компьютерных вирусов.
- Профилактика и лечение информационных инфекций.
- Программы обнаружения и защиты от вирусов.

## 10.Методические рекомендации для преподавателя

Основное внимание при изучении дисциплины «Методы и средства защиты компьютерной информации» следует уделять основным понятиям, относящимися к области защиты компьютерной информации в технических системах управления, современным методам шифрования в криптографии информационных потоков технических систем управления, программно-аппаратным комплексам защиты компьютерной информации, основным классификационными признаками компьютерных вирусов и методами защиты от них, стандартам и спецификациям в области информационной безопасности систем управления.Для активизации учебного процесса при изучении дисциплины эффективно применение презентаций по различным темам лекций.Для проведения занятий по дисциплине используются средства обучения:

- учебники, текст лекций, информационные ресурсы Интернета;

- справочные материалы и нормативно-техническая документация.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **09.03.01 «Информатика и вычислительная техника»,** образовательная программа (профиль)**Электронные системы управления.**

Приложение 1

**Структура и содержание дисциплины «Методы и средства защиты компьютерной информации» по направлению 09.03.01 «Информатика и вычислительная техника» и профилю подготовки «Электронные системы управления»**

| № № n/n | Раздел | Семестр | Неделя семестра | Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах | | | | | Виды самостоятельной работы Студентов | | | | Формы аттестации | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Л | П/С | Лаб | СРС | КСР | ПР | ДС | УО | Т(Р) | Э | З |
| **Семестр 7** | | | | | | | | | | | | | | |
| **1.1** | **Введение.** Основные понятия, положения и определения. Предмет и объект защиты. Понятие угрозы безопасности. Классификация угроз. Классификация злоумышленников. Основные методы реализации угроз информационной безопасности. Причины, виды и каналы утечки информации. | **7** | **1** | **4** | | | **4** | | | | | | | |
| **1.2** | *Лабораторная работа. Защита информации в комбинационных устройствах* | **7** | **2** | | | **4** | **4** | | | | | | | |
| **1.3** | **Правовые и организационные методы защиты компьютерной информации.** Правовое регулирование в области безопасности информации. Государственная политика РФ в области безопасности информационных технологий. Законодательная база в | **7** | **3** | **4** | | | **4** | | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | области информационных технологий. Структура государственных органов, обеспечивающих безопасность информационных технологий. Общая характеристика организационных методов защиты | | | | | | | | | | | | | |
| **1.4** | **Стандарты и спецификации в области информационной безопасности.** Общие критерии безопасности. Подготовка и целевая направленность общих критериев. Организация общих критериев. Возможности и применимость, концепции общих критериев. Действующие стандарты и рекомендации в области информационной безопасности. Критерии оценки надежных компьютерных систем («Оранжевая книга» Министерства обороны США). Гармонизированные критерии европейских стран. Руководящие документы по защите от несанкционированного доступа Гостехкомиссии при президенте РФ. Особенности информационной безопасности компьютерных сетей. Рекомендации X.800. | **7** | **4** | **4** | | | **4** | | | | | | | |
| **1.5** | **Административный уровень информационной безопасности в информационно-вычислительной системе.** Понятие политики безопасности**.** Анализ риска.Угрозы/видимость. Уязвимость/последствия. Учет информационных ценностей. Модели основных типов политик безопасности. Типы политик безопасности. Модель матрицы доступов Харрисон-Руззо- | **7** | **5** | **4** | | | **4** | | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ульмана. Модель распространения прав доступа Take-Grant. Модель системы безопасности Белла-Лападула. Модель Low-Water-Mark. Модель ролевого разграничения доступа. | | | | | | | | | | | | | |
| **1.6** | **Административный уровень информационной безопасности в информационно-вычислительной системе.** Понятие политики безопасности**.** Анализ риска.Угрозы/видимость. Уязвимость/последствия. Учет информационных ценностей. Модели основных типов политик безопасности. Типы политик безопасности. Модель матрицы доступов Харрисон-Руззо-Ульмана. Модель распространения прав доступа Take-Grant. Модель системы безопасности Белла-Лападула. Модель Low-Water-Mark. Модель ролевого разграничения доступа. | **7** | **6** | **4** | | | **4** | | | | | | | |
| **1.7** | **Криптографическая защита информации.**Основные определения криптологии. Классификация методов криптографического закрытия информации. Основы теории К. Шеннона. Основные криптографические модели. Алгоритмы шифрования. Симметричные методы шифрования. Асимметричные методы шифрования. Сравнение криптографических методов. Методы кодирования. Другие методы | **7** | **7** | **4** | | | **4** | | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1.8** | *Лабораторная работа. Защита информации методом сигнатурного анализа. Выдача заданий для рефератов* | **7** | **8** | | | **4** | **4** | | | | | + | | |
| **1.9** | **Защита компьютерной информации в локальных ЭВМ иинформационно-вычислительных сетях.**Модели безопасности основных операционных систем. Механизмы защиты операционных систем. Система безопасности WindowsNT. Защита в операционной системе NovellNetware. | **7** | **9** | **4** | | | **4** | | | | | + | | |
| **1.10** | **Системы защиты программного обеспечения.**Классификация систем защиты программного обеспечения. Достоинства и недостатки основных систем защиты. Упаковщики/шифраторы. Системы защиты от несанкционированного копирования. Системы защиты от несанкционированного доступа. Показатели эффективности систем защиты. | **7** | **10** | **4** | | | **4** | | | | | + | | |
| **1.11** | **Защита информации в корпоративных сетях.**Основы и цель политики безопасности в компьютерных сетях. Управление доступом. Идентификация и установление подлинности. Проверка полномочий субъектов на доступ к ресурсам. Регистрация обращений к защищаемым ресурсам. Реагирование на несанкционированные действия. Многоуровневая защита корпоративных сетей. Аутентификация. Анализ возможностей маршрутизации и прокси-серверов. Типы межсетевых экранов. | **7** | **11** | **2** | | | **4** | | | | | + | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1.12** | **Защита от информационных инфекций. Вирусология.** Классификация компьютерных вирусов. Профилактика и лечение информационных инфекций. Программы обнаружения и защиты от вирусов. | **7** | **12** | **2** | | | **4** | | | | | + | | |
| **1.13** | *Лабораторная работа. Защита информации методом кода Хемминга.* | **7** | **13** | | | 4 | **4** | | | | | | | |
| **1.14** | *Лабораторная работа. Защита информации в конечных автоматах.* | **7** | **14** | | | 4 | **4** | | | | | | | |
| **1.15** | *Лабораторная работа. Простые шифры.* | **7** | **15** | | | 4 | **4** | | | | | | | |
| **1.16** | *Лабораторная работа. Основы блочного шифрования.* | **7** | **16** | | | 4 | **4** | | | | | | | |
| **1.17** | *Лабораторная работа. Алгоритмы асимметричного шифрования.* | **7** | **17** | | | 4 | 4 | | | | | | | |
| **1.18** | *Лабораторная работа. Алгоритмы электронной цифровой подписи.Прием Отчетов.* | **7** | **18** | | | 4 | 4 | | | | | | | |
| **1.19** | Итоговое занятие.<br>Прием и защита лабораторных работ, докладов (презентаций), рефератов. | **7** | **18** | | | 4 | | | | | | | | |
| **1.20** | **Форма аттестации** | | | | | | | | | | | | | **З** |
| **1.21** | **Всего часов по дисциплине** | **7** | | **36** | | **36** | **72** | | | | | | | |

Приложение 1
к рабочей программе

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(МОСКОВСКИЙ ПОЛИТЕХ)**

Направление подготовки: **09.03.01 «Информатика и вычислительная техника»**
ОП (профиль): «Киберфизические системы»
Форма обучения: очная
Вид профессиональной деятельности:
производственно-технологическая, организационно-управленческая

Кафедра «СМАРТ-технологии»

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

# ПО ДИСЦИПЛИНЕ

**Методы и средства защиты компьютерной информации в системах управления**

Состав:
1. Паспорт фонда оценочных средств
2. Описание оценочных средств:
перечень вопросов для зачета (СРС)
примерный перечень тем рефератов
примерный перечень тем докладов
перечень лабораторных работ

Москва, 2022 год

Таблица 1

**ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ**

| **МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ** | | | | | |
|---|---|---|---|---|---|
| ФГОС ВО **09.03.01 «Информатика и вычислительная техника»** | | | | | |
| В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **профессиональные компетенции**: | | | | | |
| **КОМПЕТЕНЦИИ** | | **Перечень компонентов** | **Технология формирования компетенций** | **Форма оценочного средства**** | **Степени уровней освоения компетенций** |
| **ИНДЕКС** | **ФОРМУЛИРОВКА** | | | | |
| **ОПК-1** | Способностью применять естественно-научные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности | **знать:**<br>● о методах математического анализа и моделирования. Знать основную теорию об экспериментальных исследованиях в профессиональной деятельности<br>**уметь:**<br>● применять естественно-научные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности<br>**владеть:** | лекция, самостоятельная работа, лабораторные работы, рефераты, доклады-сообщения, презентации | ДС,<br>Р,<br>УО,<br>Пр,<br>ЛР | **Базовый уровень:**<br>воспроизводство полученных знаний в ходе текущего контроля; умение решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам<br>**Повышенный уровень:**<br>практическое применение полученных знаний в процессе изучения дисциплины; готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном |

| | | | | | |
|---|---|---|---|---|---|
| | | ● навыками применения полученных знаний и навыками общеинженерного моделирования<br>● умениями проводить экспериментальные исследования | | | и методическом обеспечении |
| ОПК-2 | способностью использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности | **знать:**<br>● о теорию о самых современных информационных технологиях и программных средствах, методах их применения в профессиональной деятельности<br>**уметь:**<br>● использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности<br>**владеть:**<br>● навыками применения самых современных информационных технологий и программных средств в решении поставленной задачи | лекция, самостоятельная работа, лабораторные работы, рефераты, доклады-сообщения, презентации | ДС,<br>Р,<br>УО,<br>Пр,<br>ЛР | **Базовый уровень:**<br>воспроизводство полученных знаний в ходе текущего контроля; умение решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам<br>**Повышенный уровень:**<br>практическое применение полученных знаний в процессе изучения дисциплины; готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | определенности, при недостаточном документальном, нормативном и методическом обеспечении |
| ОПК-9 | Способностью осваивать методики использования программных средств для решения практических задач | **знать:**<br>● о методиках использования программных средств для решения практических задач<br>**уметь:**<br>● на практике применять освоенные методики использования программных средств для решения практических задач<br>**владеть:**<br>● навыками освоения различных методик, с помощью которых можно использовать программные средства | лекция, самостоятельная работа, лабораторные работы, рефераты, доклады-сообщения, презентации | ДС,<br>Р,<br>УО,<br>Пр,<br>ЛР | **Базовый уровень:**<br>воспроизводство полученных знаний в ходе текущего контроля; умение решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам<br>**Повышенный уровень:**<br>практическое применение полученных знаний в процессе изучения дисциплины; готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении |
| ПК-2 | Способностью разрабатывать требования и проектировать программное обеспечение | **знать:**<br>● основные принципы написания программного кода, алгоритма<br>**уметь:** | лекция, самостоятельная работа, лабораторные работы, рефераты, | ДС,<br>Р,<br>УО,<br>Пр,<br>ЛР | **Базовый уровень:**<br>воспроизводство полученных знаний в ходе текущего контроля; умение решать типовые задачи, принимать профессиональные и |

| | | | | | |
|---|---|---|---|---|---|
| | | ● оперировать командами языка программирования и писать код, разрабатывать алгоритм, необходимы для решения поставленной задачи<br>**владеть:**<br>● навыками решения поставленных задач, знаниями об используемом языке программирования | доклады-сообщения, презентации | | управленческие решения по известным алгоритмам, правилам и методикам<br>**Повышенный уровень:**<br>практическое применение полученных знаний в процессе изучения дисциплины; готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении |

**- Сокращения форм оценочных средств см. в приложении 2 к РП.

**Перечень оценочных средств по дисциплине**

**Методы и средства защиты компьютерной информации**

| № ОС | Наименование оценочногосредства | Краткая характеристика оценочного средства | Представление оценочного средства в ФОС |
|---|---|---|---|
| 1 | Доклад, сообщение (ДС) | Продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научнойтемы | Темыдокладов, сообщений |
| 2 | Устный опрос/ собеседование, (УО) | Средство контроля, организованное как специальная беседа педагогического работника с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. | Вопросы по темам/разделам дисциплины |
| 3 | Реферат (Р) | Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического** ан анализа | Темы рефератов |
| 4 | Презентация (ПР) | Представление студентом наработанной информации по заданной тематике в виде набора слайдов и спецэффектов, подготовленных в выбранной программе | Темы презентаций |
| 5 | Лабораторные работы (ЛР) | Оценка способности студента применить полученные ранее знания для проведения анализа, опыта, эксперимента и выполнения последующих расчетов, а также составления выводов | Перечень лабораторных работ и их оснащение |

****** - анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.

**Перечень вопросов к зачету (Код компетенции ОПК-3; ОПК-9)**

-Криптографическая защита информации**.**Основные определения криптологии.
- Классификация методов криптографического закрытия информации.
-Основы теории К. Шеннона.
- Основные криптографические модели. Алгоритмы шифрования.
-Симметричные методы шифрования.
-Асимметричные методы шифрования.
-Сравнение криптографических методов.
- Методы кодирования. Другие методы.

-Защита компьютерной информации в локальных ЭВМ и информационно-вычислительных сетях.
-Модели безопасности основных операционных систем. Механизмы защиты операционных систем.
- Система безопасности WindowsNT.
- Защита в операционной системе NovellNetware.
-Системы защиты программного обеспечения.Классификация систем защиты программного обеспечения.
-Достоинства и недостатки основных систем защиты. Упаковщики/шифраторы.
-Системы защиты от несанкционированного копирования.
- Системы защиты от несанкционированного доступа. Показатели эффективности систем защиты.
-Защита информации в корпоративных сетях.Основы и цель политики безопасности в компьютерных сетях.
- Управление доступом. Идентификация и установление подлинности.
-Проверка полномочий субъектов на доступ к ресурсам. Регистрация обращений к защищаемым ресурсам.
- Реагирование на несанкционированные действия.
- Многоуровневая защита корпоративных сетей. Аутентификация.
- Анализ возможностей маршрутизации и прокси-серверов.
-Типы межсетевых экранов.
-Защита от информационных инфекций. Вирусология.
-Классификация компьютерных вирусов.
- Профилактика и лечение информационных инфекций.
- Программы обнаружения и защиты от вирусов.
-Основные понятия, положения и определения защиты информации в информационно-вычислительных системах.
-Предмет и объект защиты. Понятие угрозы безопасности.
-Классификация угроз. Классификация злоумышленников.
- Основные методы реализации угроз информационной безопасности.
-Причины, виды и каналы утечки информации.
-Правовые и организационные методы защиты компьютерной информации.
-Правовое регулирование в области безопасности информации.
-Государственная политика РФ в области безопасности информационных технологий.
-Законодательная база в области информационных технологий.
- Структура государственных органов, обеспечивающих безопасность информационных технологий.
- Общая характеристика организационных методов защиты.
-Стандарты и спецификации в области информационной безопасности.
-Общие критерии безопасности. Подготовка и целевая направленность общих критериев.
-Организация общих критериев. Возможности и применимость, концепции общих критериев.
- Действующие стандарты и рекомендации в области информационной безопасности.
-Критерии оценки надежных компьютерных систем («Оранжевая книга» Министерства обороны США).
- Гармонизированные критерии европейских стран.
- Руководящие документы по защите от несанкционированного доступа Гостехкомиссии при президенте РФ.
- Особенности информационной безопасности компьютерных сетей. Рекомендации X.800.
-Административный уровень информационной безопасности в информационно-вычислительной системе.

-Понятие политики безопасности**.** Анализ риска.Угрозы/видимость. Уязвимость/последствия.
-Учет информационных ценностей. Модели основных типов политик безопасности.
-Типы политик безопасности. Модель матрицы доступов Харрисон-Руззо-Ульмана.
-Модель распространения прав доступа Take-Grant.
-Модель системы безопасности Белла-Лападула.
- Модель Low-Water-Mark.
- Модель ролевого разграничения доступа.

**ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ РЕФЕРАТОВ ПО ДИСЦИПЛИНЕ «МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ » (КОД КОМПЕТЕНЦИИ ОПК-3;ОПК – 9)**

1. Определение информации, ее классификация. Основные определения и термины при защите информации.
2. Основные термины криптографии.
3. Методы шифрования в криптографии: перестановок, замены, гаммирования.
4. Методы стеганографии в защите информации.
5. Хеш-функции в задачах защиты информации.
6. Аппаратные и программные методы и средства защиты информации при электронной обработке данных.
7. Аппаратные и программные методы и средства парольной защиты.
8. Атаки на протоколы идентификации.
9. Методы «запрос-ответ» при идентификации. Биометрическая идентификация.
10. Основные определения и механизмы информационной безопасности.
11. Система охраны периметра траектории с компьютерными системами.
12. Система видеонаблюдения для обеспечения информационной безопасности.
13. Назначение и роль охранной (пожарной) сигнализации в защите информации.
14. Назначение и сущность цифровой подписи.
15. Межсетевые экраны с контролем соединений.
16. Атаки некорректными сетевыми пакетами типа Nuke. Защита протоколов сетевой безопасности.
17. Основные методы информационной безопасности.
18. Dos-атаки. Методы защиты.
19. Понятие компьютерного вируса. Признаки. Методы обнаружения. Способы борьбы.
20. Методы защиты от компьютерных вирусов.
21. Автоматизированные средства безопасности. Антивирусы.
22. Методы удаления последствий заражения компьютерными вирусами.
23. Основные механизмы ввода пароля.

**24.** Угрозы преодоления парольной защиты.

**25.** Защита от атак на web-сайты и web-браузеры.

**26.** Сигнатурный метод защиты информации при сетевых атаках типа Teardrop.

## ПЕРЕЧЕНЬ ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНЕ «МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ» (КОД КОМПЕТЕНЦИИ ОПК-3; ОПК – 9)

Защита комбинационных устройств.
Защита информации с применением кода Хэмминга.
Защита конечных автоматов.
Защита информации методом сигнатурного анализа.
Защита от сбоев аппаратными средствами.
Простые шифры.
Основы блочного шифрования.
Алгоритмы асимметричного шифрования.
Алгоритмы электронной цифровой подписи.

## ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ ДОКЛАДОВ (ПРЕЗЕНТАЦИЙ) ПО ДИСЦИПЛИНЕ «МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ» (КОД КОМПЕТЕНЦИИ ОПК-3; ОПК – 9)

**1.** Автоматизированный комплекс для оценки состояния технических систем со скрытыми отказами.

**2.** Технологии компьютерного моделирования.

**3.** Разработка среды визуального моделирования и анализа потоковых систем на основе квазиклеточных сетей.

**4.** Интеллектуальная защита от сбоев устройств связи с объектом.

**5.** ГОСТ 28147-89 системы обработки информации. Защита криптографическая.

**6.** Интеллектуальная защита от сбоев в сетях Wi-Fi.

**7.** Кибербезопасность технической документации в СУ.

**8.** Компьютерные вирусы. Способы распространения вирусов. Антивирусные программы.

**9.** Электромагнитная совместимость (ЭМС). Кондуктивные помехи по цепям питания (ГОСТ 28751-90).

**10.** ЭМ-защита электрооборудования автомобиля и автомобильной бортовой радиоэлектронной аппаратуры (ГОСТ 28279-89).

**11.** ГОСТ 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении».

**12.** Электронная защита систем управления.

**13.** Защиты компьютерной информации космических аппаратов.

**14.** Контрольно-измерительный оптико-электронный комплекс (ОЭК) для наблюдения за ближним и дальним космосом (на базе ОЭК «Окно»).

**15.** Методы и средства обеспечения информационной безопасности в беспроводных сетях типа IOT.

**16.** Автоматизация бизнес-процессов внутреннего документооборота предприятия.

**17.** Алгоритмы защиты электроосветительного оборудования в авиационной автоматизированной системе.

**18.** Верификация сбоев в СУ: а)на стадии проектирования; б)на стадии эксплуатации.

**19.** Информативные признаки аппаратных сбоев в СУ.

**20.** Дифференциальные сбои в СУ.

**21.** Интегральные сбои в СУ.

**22.** Интегро-дифференциальные сбои в СУ.

**23.** Комбинированные сбои в СУ.

**24.** Многократные сбои в СУ.

**25.** Гибридные методы при диагностике сбоев в СУ.

**26.** Мажоритарные методы при диагностике сбоев в СУ.

27. Интеллектуальная защита от отказов и сбоев в СУ методом тестовых кодов (код Вьюшкова – Дианова).