**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ**
**РОССИЙСКОЙ ФЕДЕРАЦИИ**
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета _____ С.М. Пасмурнов
«31» августа 2017 г.

# РАБОЧАЯ ПРОГРАММА
дисциплины
«Теория управления информационной безопасностью распределённых компьютерных систем»

**Специальность** 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

**Специализация**

**Квалификация выпускника** специалист по защите информации

**Нормативный период обучения** 5 лет и 6 м.

**Форма обучения** очная

**Год начала подготовки** 2016

Автор программы _____/К.А. Разинкин/

Заведующий кафедрой
Систем информационной
безопасности _____/ А.Г. Остапенко /

Руководитель ОПОП _____/ А.Г. Остапенко /

Воронеж 2017

## 1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

**1.1.Целидисциплины**является исследование подходов к анализу и синтезу систем автоматического управления в технических системах, а также изучение методов и средств управления информационной безопасностью распределенных компьютерных систем, изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию технологий распределенных компьютерных систем

**1.2.Задачиосвоениядисциплины**

изучение основных понятий, методов, моделей и алгоритмов анализа и синтеза непрерывных и дискретных систем автоматического регулирования во временном и частотном диапазонах;

обучение студентов систематизированным представлениям о принципах построения, функционирования и применения распределенных компьютерных систем;

обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ организации;

освоение принципов построения и алгоритмов функционирования защищенных приложений компьютерных систем, принципов построения и алгоритмов функционирования их подсистем защиты информации.

## 2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Теорияуправленияинформационнойбезопасностьюраспределённыхкомпьютерныхсистем»относитсякдисциплинамбазовойчастиблокаБ1.

## 3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Теорияуправленияинформационнойбезопасностьюраспределённыхкомпьютерныхсистем»направленаформирование следующихкомпетенций:

ПК-2-способностьюучаствоватьвтеоретическихиэкспериментальныхнаучно-исследовательскихработахпооценкезащищенностиинформациивкомпьютерныхсистемах,составлятьнаучныеотчеты,обзорыпорезультатамвыполненияисследований

ПК-12-способностьюпроводитьинструментальныймониторингзащищенностикомпьютерныхсистем

ПК-15-способностьюразрабатыватьпредложенияпосовершенствованию системыуправленияинформационнойбезопасностьюкомпьютернойсистемы

| Компетенция | Результатыобучения,характеризующие сформированностькомпетенции |
|---|---|
| ПК-2 | знать основные принципы построения защищенных распределенных компьютерных систем; способы обнаружения и нейтрализации последствий |

| | |
|---|---|
| | вторжений в компьютерные системы |
| | уметь формализовать задачу управления безопасностью информационных систем; анализировать защищенность компьютерных систем |
| ПК-12 | знать принципы построения СУИБ и, в её рамках, разработки процессов управления ИБ |
| | уметь анализировать состояние ИБ на предприятии в динамике с целью разработки требований к разрабатываемым процессам управления ИБ |
| | владеть навыками выявления и устранения уязвимостей компьютерной сети; - навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем |
| ПК-15 | знать основные понятия и последовательность этапов решения задачи управления необходимых для совершенствования системы управления информационной безопасностью компьютерной системы |
| | уметь использовать математический аппарат, необходимый для решения конкретной задачи управления в рамках динамической системы управления безопасностью компьютерной системы |
| | владеть методиками построения линейных систем управления информационной безопасностью компьютерной системы и их реализациями в современных инструментальных средах автоматизации инженерных и научных расчётов |

## 4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Теорияуправленияинформационнойбезопасностьюраспределённыхкомпьютерныхсистем»составляет6з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

**очнаяформаобучения**

| Видыучебнойработы | Всего часов | Семестры | |
|---|---|---|---|
| | | 8 | 9 |
| **Аудиторныезанятия (всего)** | 108 | 54 | 54 |
| В томчисле: | | | |

| | | | |
|---|---|---|---|
| Лекции | 72 | 36 | 36 |
| Практическиезанятия (ПЗ) | 36 | 18 | 18 |
| **Самостоятельнаяработа** | 72 | 18 | 54 |
| **Курсовойпроект** | + | + | |
| Часынаконтроль | 36 | - | 36 |
| Виды промежуточной аттестации - экзамен, зачет с оценкой | + | + | + |
| Общая трудоемкость:<br>академические часы<br>зач.ед. | 216<br>6 | 72<br>2 | 144<br>4 |

## 5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

### 5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

### очнаяформаобучения

| № п/п | Наименованиетемы | Содержаниераздела | Лекц | Прак зан. | СРС | Всего, час |
|---|---|---|---|---|---|---|
| 1 | Введение в теорию автоматического управления. Непрерывные системы управления. | Роль и место дисциплины в программе подготовки специалиста. Дифференциальные уравнения физических систем. Статические и динамические характеристики систем. Линеаризация характеристик заданных графически и аналитически. Импульсная (весовая) и переходная функции. Преобразование Лапласа. Уравнение переходного процесса. Передаточные функции линейных систем. Типовые динамические звенья. Структурные схемы. Модели в переменных состояния. Модели систем в переменных состояния в виде сигнальных графов. Связь между передаточной функцией и уравнениями состояния. Временные характеристики и переходная матрица состояния. Анализ моделей в переменных состояния с помощью MATLAB. | 12 | 6 | 12 | 30 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Определение устойчивости по А.М.Ляпунову. Алгебраические критерии устойчивости систем автоматического управления. Частотные критерии устойчивости систем автоматического управления. Построение областей устойчивости в плоскости параметров системы автоматического управления. D–разбиение. Понятие качества регулирования. Прямые показатели качества: перерегулирование, быстродействие, динамический коэффициент регулирования и т.д. Корневые методы оценки качества управления. Частотные показатели качества САУ. Трёхканальные (ПИД) регуляторы. Схемы последовательной коррекции: синтез с помощью диаграммы Боде; синтез с помощью корневого годографа. Синтез систем с применением интегрирующих устройств. Синтез систем с обратной связью по состоянию. | | | | |
| 2 | Дискретные системыуправления | Цифровые законы управления. Описание работы цифровой части. Линейные законы управления. Операторные модели. Восстановление непрерывных сигналов. Понятие экстраполятора. Анализ последовательностей Z и ζ-преобразование. Вычисление изображений. Свойства z-преобразования. Восстановление оригинала. Линейные дискретные системы. Импульсная | 12 | 6 | 12 | 30 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | характеристика. Дискретная передаточная функция. Нули и полюса. Типовые переходные процессы. Модели в пространстве состояний. Физическая реализуемость. Устойчивость. Устойчивость по А.М. Ляпунову. Устойчивость линейных систем. Алгебраические критерии устойчивости. Критерий Михайлова. Критерий Найквиста. Одноконтурнаядискретнаяс истема. Структурнаясхема. | | | | |
| 3 | Оптимальноеуправление | Постановка задачи управления. Функционал, его экстремум и вариация. Простейшая задача вариационного исчисления. Уравнение Эйлера. Поле экстремалей. Задача с подвижными границами. Доказательство принципа максимума для простейшей задачи терминального управления. Принцип максимума для нелинейных систем. Схема решения задач оптимального управления с помощью принципа максимума. Условия трансверсальности при различных режимах на концах оптимальной траектории. Задача с квадратичным функционалом. Принцип максимума для дискретных задач. Примеры решения задач. Динамическое программирование для линейной системы с квадратичным функционалом. Метод динамического программирования для нелинейных систем. Схема Беллмана для дискретных задач. Примеры решения | 12 | 6 | 12 | 30 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | задач с помощью метода Беллмана: задача о распределении ресурсов, о замене оборудования и т.д. | | | | |
| 4 | Основыуправления ИБ | Цели и задачи управления ИБ. Стандартизация в области управления ИБ Системы управления ИБ. Процессный подход. Место СУИБ в рамках общей системы управления. Область деятельности СУИБ. Ролевая структура СУИБ. Понятие роли. Использование ролевого принципа в рамках СУИБ. Политика СУИБ. Цели Политики СУИБ. Управление безопасностью каналов передачи информации в распределенных компьютерных и инфокоммуникационных системах. Правила синтеза адаптивных алгоритмов, динамическое управление их параметрами в процессе реализации целевых функций информационного воздействия, элементов защищаемой системы и, собственно, системы. Рациональный, рефлексивный и адаптивный алгоритмы управления. Требование по обеспечению контроля в отношении логического доступа. Контроль в отношении доступа пользователей. Обязанности пользователей. Контроль сетевого доступа. Контроль доступа к операционной системе. Контроль доступа к приложениям. Мониторинг доступа и использования системы. **ActiveDirectory.** Управление учетными записями. Доверительные | 12 | 6 | 12 | 30 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | отношения. Инструменты администрирования. Групповая политика. Расширяемость. Разделение физической сети. **OpenLDAP.** Открытая реализация LDAP. История появления OpenLDAP. ОсновныекомпонентыOpen LDAP. | | | | |
| 5 | Управление рисками при обеспечении информационной безопасности распределенных компьютерных систем | Область применения. Термины и определения. Стандарты в области управления рисками ИБ. Обзор процесса управления рисками ИБ. Общие положения. Основные критерии. Общее описание оценки риска ИБ. Анализ риска. Оценка риска. Общее описание обработки риска. Снижение риска. Сохранение риска. Предотвращение риска. Перенос риска. Принятие риска ИБ. Коммуникация риска ИБ. Мониторинг и переоценка факторов риска. Мониторинг, анализ и улучшение управления рисками. Примеры типичных угроз. Уязвимости и методы оценки уязвимостей. Подходы к оценке риска ИБ. | 12 | 6 | 12 | 30 |
| 6 | Администрирование средств безопасности | Управление ключами (генерация и распределение). Управление шифрованием (установка и синхронизация криптографических параметров). Администрирование управления доступом (распределение информации, необходимой для управления - паролей, списков доступа и т.п.). Управление аутентификацией (распределение информации, необходимой | 12 | 6 | 12 | 30 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | для аутентификации - паролей, ключей и т.п.). Управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений - частоту отправки, размер и т.п.). Управление маршрутизацией(выделение доверенных путей). Управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб). | | | | |
| | | **Итого** | **72** | **36** | **72** | **180** |

**5.2Перечьлабораторныхработ**

Непредусмотреноучебнымпланом

## 6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплиныпредусматриваетвыполнениекурсовогопроектав8семестредляочнойформыобучения.

Примерная тематика курсового проекта: «Анализ работоспособности непрерывных систем автоматического управления»

Задачи, решаемые при выполнении курсового проекта:

• получить навыки анализа непрерывной САР на устойчивость;

• получить навыки анализа непрерывной САР на качество регулирования

• получить навыки коррекции САР.

Курсовойпроектвключатвсебяграфическуючастьирасчетно-пояснительнуюзаписку.

## 7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

### 7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

#### 7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

| Компе-тенция | Результатыобучения,характеризующие сформированностькомпетенции | Критерии оценивания | Аттестован | Неаттестован |
|---|---|---|---|---|
| ПК-2 | знать основные принципы построения защищенных распределенных компьютерных систем; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы | знание основных принципов построения защищенных распределенных компьютерных систем и способов обнаружения и нейтрализации последствий вторжений в компьютерные системы | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | уметь формализовать задачу управления безопасностью информационных систем; анализировать защищенность компьютерных систем | умение формализовать задачу управления безопасностью информационных систем, а также умение анализировать защищенность компьютерных систем | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ПК-12 | знать принципы построения СУИБ и, в её рамках, разработки процессов управления ИБ | знание принципы построения СУИБ и особенности отдельных процессов управления в рамках СУИБ | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | уметь анализировать состояние ИБ на предприятии в динамике с целью разработки требований к разрабатываемым процессам управления ИБ | умение анализировать текущее состояние ИБ, применять процессный подход к управлению ИБ в различных сферах деятельности | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | владеть навыками выявления и устранения уязвимостей компьютерной сети; - навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем | владение навыками анализа бизнес-активов организации, угроз и рисков ИБ, уязвимостей в рамках области действия СУИБ | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ПК-15 | знать основные понятия и последовательность этапов решения задачи управления необходимых для | знаниеосновных понятий и последовательности этапов решения задачи управления необходимых для | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

| | | | | |
|---|---|---|---|---|
| | совершенствования системы управления информационной безопасностью компьютерной системы | совершенствования системы управления информационной безопасностью компьютерной системы | | |
| | уметь использовать математический аппарат, необходимый для решения конкретной задачи управления в рамках динамической системы управления безопасностью компьютерной системы | используя современные методы и средства, разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | владеть методиками построения линейных систем управления информационной безопасностью компьютерной системы и их реализациями в современных инструментальных средах автоматизации инженерных и научных расчётов | владение навыками построения как отдельных процессов управления и системы процессов в целом. | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

**7.1.2Этаппромежуточногоконтролязнаний**

Результатыпромежуточногоконтролязнанийоцениваютсяв8,9семестредляочнойформыобученияпочетырехбалльнойсистеме:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

| **Компе-тенция** | **Результатыобучения,характеризующие сформированностькомпетенции** | **Критерии оценивания** | **Отлично** | **Хорошо** | **Удовл.** | **Неудовл.** |
|---|---|---|---|---|---|---|
| ПК-2 | знать основные принципы построения защищенных распределенных компьютерных систем; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы | Тест | Выполнениетестана 90-100% | Выполнениетестана 80- 90% | Выполнение тестана 70-80% | В тесте менее 70% правильных ответов |

| | | | | | | |
|---|---|---|---|---|---|---|
| | уметь формализовать задачу управления безопасностью информационных систем; анализировать защищенность компьютерных систем | Решениест андартных практическ ихзадач | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачине решены |
| ПК-12 | знать принципы построения СУИБ и, в её рамках, разработки процессов управления ИБ | Тест | Выполнениетеста на 90-100% | Выполнениетестана 80- 90% | Выполнение тестана 70-80% | В тесте менее 70% правильных ответов |
| | уметь анализировать состояние ИБ на предприятии в динамике с целью разработки требований к разрабатываемым процессам управления ИБ | Решениест андартных практическ ихзадач | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачине решены |
| | владеть навыками выявления и устранения уязвимостей компьютерной сети; - навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачине решены |
| ПК-15 | знать основные понятия и последовательность этапов решения задачи управления необходимых для совершенствования системы управления информационной безопасностью компьютерной системы | Тест | Выполнениетеста на 90-100% | Выполнениетестана 80- 90% | Выполнение тестана 70-80% | В тесте менее 70% правильных ответов |
| | уметь использовать математический аппарат, необходимый для решения конкретной задачи управления в рамках динамической системы управления | Решениест андартных практическ ихзадач | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во | Продемонстрирован верный ход решения в большинстве задач | Задачине решены |

| | | | | | | |
|---|---|---|---|---|---|---|
| | безопасностью компьютерной системы | | | всех задачах | | |
| | владеть методиками построения линейных систем управления информационной безопасностью компьютерной системы и их реализациями в современных инструментальных средах автоматизации инженерных и научных расчётов | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачине решены |

**7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияилиныематериалы,необходимыедляоценкизнаний,умений,навыкови(или)опытадеятельности)**

**7.2.1Примерныйпереченьзаданийдляподготовкиктестированию**

*(минимум10вопросовдлятестированиясвариантамиответов)*

1.УПРАВЛЕНИЕ БЕЗ НЕПОСРЕДСТВЕННОГО УЧАСТИЯ ЧЕЛОВЕКА НАЗЫВАЕТСЯ:

**A) дистанционным;**

B) автоматизированным;

C) автоматическим;

D) телемеханическим;

E) централизованным.

2.УПРАВЛЕНИЕ С ЧАСТИЧНЫМ УЧАСТИЕМ ЧЕЛОВЕКА НАЗЫВАЕТСЯ:

A) дистанционным;

**B) автоматизированным;**

C) автоматическим;

D) телемеханическим;

E) централизованным.

**3.**УПРАВЛЕНИЕ БЕЗ УЧАСТИЯ ЧЕЛОВЕКА НАЗЫВАЕТСЯ:

A) дистанционным;

B) автоматизированным;

**C) автоматическим;**

D) телемеханическим;

E) централизованным.

**4.**ЗАМКНУТОЙ СИСТЕМОЙ ПО ОТКЛОНЕНИЮ НАЗЫВАЕТСЯ ТАКАЯ СИСТЕМА, В КОТОРОЙ:

A) на вход автоматического регулятора поступает сумма задающего и возмущающего воздействий;

B) на вход автоматического регулятора поступает сумма нескольких задающих воздействий с разными знаками;

**C) на вход автоматического регулятора поступает разность**

**задающего воздействия и выходной величины;**

D) на вход автоматического регулятора поступает сумма задающего, возмущающего воздействий и выходной величины;

E) на вход автоматического регулятора поступает задающее воздействие.

**5.**РАЗОМКНУТОЙ СИСТЕМОЙ ПЕРВОГО РОДА НАЗЫВАЕТСЯ ТАКАЯ СИСТЕМА, В КОТОРОЙ:

A) на вход автоматического регулятора поступает сумма задающего и возмущающего воздействий;

B) на вход автоматического регулятора поступает сумма нескольких задающих воздействий с разными знаками;

C) на вход автоматического регулятора поступает разность задающего воздействия и выходной величины;

D) на вход автоматического регулятора поступает сумма задающего, возмущающего воздействий и выходной величины;

**E) на вход автоматического регулятора поступает задающее воздействие.**

**6.**РАЗОМКНУТОЙ СИСТЕМОЙ ВТОРОГО РОДА НАЗЫВАЕТСЯ ТАКАЯ СИСТЕМА, В КОТОРОЙ:

**A) на вход автоматического регулятора поступает сумма задающего и возмущающего воздействий;**

B) на вход автоматического регулятора поступает сумма нескольких задающих воздействий с разными знаками;

C) на вход автоматического регулятора поступает разность задающего воздействия и выходной величины;

D) на вход автоматического регулятора поступает сумма задающего, возмущающего воздействий и выходной величины;

E) на вход автоматического регулятора поступает задающее воздействие.

**7.**СИСТЕМА АВТОМАТИЧЕСКОГО РЕГУЛИРОВАНИЯ, КОТОРАЯ ХАРАКТЕРИЗУЕТСЯ ПРОИЗВОЛЬНЫМ ЗАКОНОМ ИЗМЕНЕНИЯ ЗАДАЮЩЕГО ВОЗДЕЙСТВИЯ ВО ВРЕМЕНИ, НАЗЫВАЕТСЯ:

**A) следящей;**

B) статической;

C) астатической;

D) программной;

E) системой стабилизации.

8.СИСТЕМА АВТОМАТИЧЕСКОГО РЕГУЛИРОВАНИЯ, В КОТОРОЙ ЗАДАЮЩЕЕ ВОЗДЕЙСТВИЕ ПОСТОЯННО ВО ВРЕМЕНИ, НАЗЫВАЕТСЯ:

A) следящей;

B) статической;

C) астатической;

D) программной;

**E) системой стабилизации.**

**9.**СИСТЕМА АВТОМАТИЧЕСКОГО РЕГУЛИРОВАНИЯ, В КОТОРОЙ ЗАДАЮЩЕЕ ВОЗДЕЙСТВИЕ ИЗМЕНЯЕТСЯ ПО ЗАРАНЕЕ ЗАДАННОМУ ЗАКОНУ, НАЗЫВАЕТСЯ:

A) следящей;

B) статической;

C) астатической;

**D) программной;**

E) системой стабилизации.

**10.**СИСТЕМОЙ СТАБИЛИЗАЦИИ НАЗЫВАЕТСЯ:

A) автоматическая система, в которой отсутствует обратная связь;

**B) автоматическая система, в которой задающее воздействие постоянно;**

C) автоматическая система, в которой задающее воздействие изменяется по заранее заданному закону;

D) автоматическая система, на которую не воздействуют внешние возмущающие воздействия;

E) автоматическая система, в которой задающее воздействие изменяется по случайному закону.

**11.**НЕЛИНЕЙНОЙ НАЗЫВАЕТСЯ ТАКАЯ СИСТЕМА АВТОМАТИЧЕСКОГО РЕГУЛИРОВАНИЯ:

A) которая обладает способностью приспосабливаться к изменению внешних условий;

B) все параметры которой изменяются во времени;

C) которая описывается линейными дифференциальными уравнениями любого порядка;

D) в которой все звенья описываются уравнениями вида y=kx;

**E) в состав которой входит хотя бы одно звено, описываемое нелинейными уравнениями**

12.ИМПУЛЬСНОЙ НАЗЫВАЕТСЯ ТАКАЯ СИСТЕМА АВТОМАТИЧЕСКОГО РЕГУЛИРОВАНИЯ:

A) которая обладает способностью приспосабливаться к изменению внешних условий;

B) все параметры которой изменяются во времени;

C) которая описывается линейными дифференциальными уравнениями любого порядка;

**D) в состав которой входит хотя бы одно импульсное звено;**

E) в состав которой входит хотя бы одно звено, описываемое уравнениями вида y=kx.

**13.**РЕЛЕЙНОЙ НАЗЫВАЕТСЯ ТАКАЯ СИСТЕМА АВТОМАТИЧЕСКОГО РЕГУЛИРОВАНИЯ:

A) которая обладает способностью приспосабливаться к изменению внешних условий;

**B) в состав которой входит хотя бы одно релейное звено;**

C) которая описывается линейными дифференциальными уравнениями любого порядка;

D) в состав которой входит хотя бы звено, описываемое уравнением вида y=kx;

E) все параметры которой изменяются во времени.

14.СИСТЕМОЙ ПРЯМОГО ДЕЙСТВИЯ НАЗЫВАЕТСЯ:

A) система, в которой выходная величина изменяется прямо пропорционально входной;

B) вычислительная система с управляющим компьютером;

C) трехвходовая система;

**D) система с регулятором без дополнительного источника энергии;**

E) система с регулятором использующим дополнительный источник энергии.

15.СИСТЕМОЙ НЕПРЯМОГО ДЕЙСТВИЯ НАЗЫВАЕТСЯ:

A) система, в которой выходная величина изменяется прямо пропорционально входной;

B) вычислительная система с управляющим компьютером;

C) трехвходовая система;

D) система с регулятором без дополнительного источника энергии;

**E) система с регулятором использующим дополнительный источник энергии.**

16.ОБЪЕКТОМ РЕГУЛИРОВАНИЯ НАЗЫВАЕТСЯ:

A) устройство, совокупность устройств или часть устройства предназначенное для обеспечения заданных параметров качества процесса регулирования;

**B) устройство, совокупность устройств или часть устройства предназначенное для выполнения рабочей операции;**

C) устройство, совокупность устройств или часть устройства имеющее две входные величины;

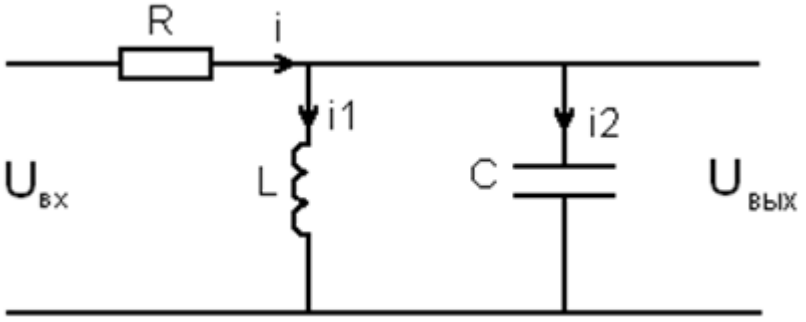
D) устройство, совокупность устройств или часть устройства выполняющее операцию сравнения входной и выходной координаты;

E) устройство, совокупность устройств или часть устройства обеспечивающее требуемые параметры качества технологического процесса

### 7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

*Пример выполнения задания*

Дана цепь. R=5; L=10;C=12




Для заданной электрической цепи составить дифференциальные уравнения. Найти передаточную функцию

$$U_c - U_{вых} = 0 \;;\; \frac{1}{C}\int i_2\,dt = U_{вых} \;;\; i_2 = C\frac{dU_{вых}}{dt};\; U_{вых} = U_L;\; L\frac{di_1}{dt} = U_{вых}$$

$$di_1 = \frac{1}{L}U_{вых}\,dt \;;\; i_1 = \frac{1}{L}\int U_{вых}\,dt \;;\; i = i_1 + i_2 = \frac{1}{L}\int U_{вых}\,dt + C\frac{dU_{вых}}{dt}$$

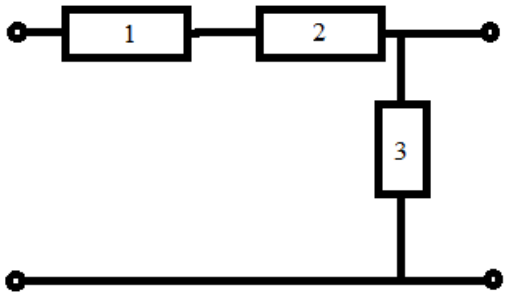
$$U_{вх} = U_R + U_L = Ri + L\frac{di_1}{dt};\; U_{вх} = R\left(\frac{1}{L}\int U_{вых}\,dt + C\frac{dU_{вых}}{dt}\right) + \frac{d\int U_{вых}\,dt}{dt}$$

При подстановке данных получаем окончательное дифференциальное уравнение: $\frac{dU_{вх}}{dt} = 60\,\frac{d^2U_{вых}}{dt^2} + \frac{dU_{вых}}{dt} + \frac{1}{2}U_{вых}$

Применим преобразование Лапласа и запишем передаточную функцию для данной цепи

$$PU_{вх}(P) = 60\,P^2U_{вых}(P) + PU_{вых}(P) + \frac{1}{2}U_{вых} \;;\; W(P) = \frac{U_{вых}(P)}{U_{вх}(P)} = \frac{P}{60\,P^2 + P + 0{,}5}$$

Дана цепь.




Записать уравнение, описывающее переходные процессы в цепи. Получить передаточную функцию.

Варианты:

| № | Обозначения |
|---|---|
| 1 | 1-R; 2-L; 3-C; |
| 2 | 1- C; 2-L; 3-R; |
| 3 | 1- C; 2-R; 3-R; |
| 4 | 1-R; 2-C; 3-R; |
| 5 | 1-L; 2-C ; 3-R; |
| 6 | 1-R; 2-L; 3-R; |
| 7 | 1- R; 2-L; 3-L; |
| 8 | 1-C; 2-C; 3-R ; |
| 9 | 1- R; 2-C;3-L; |
| 10 | 1-L; 2-C;3-C. |

**7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач**

**1) К правовым методам, обеспечивающим информационную безопасность, относятся:**

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

**2) Основными источниками угроз информационной безопасности являются все указанное в списке:**

- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

**3) Виды информационной безопасности:**

+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

**4) Цели информационной безопасности – своевременное обнаружение, предупреждение:**

+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

**5) Основные объекты информационной безопасности:**

+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

**6) Основными рисками информационной безопасности являются:**

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

**7) К основным принципам обеспечения информационной безопасности относится:**

+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

**8) Основными субъектами информационной безопасности являются:**

- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

**9) К основным функциям системы безопасности можно отнести все перечисленное:**

+ Установление регламента, аудит системы, выявление рисков

- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

**10) Принципом информационной безопасности является принцип недопущения:**

+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

**11) Принципом политики информационной безопасности является принцип:**

+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

**12) Принципом политики информационной безопасности является принцип:**

+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

**13) Принципом политики информационной безопасности является принцип:**

+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

**14) К основным типам средств воздействия на компьютерную сеть относится:**

- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания

**15)Угроза информационной системе (компьютерной сети) – это:**

+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

**16) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:**

- Регламентированной
- Правовой
+ Защищаемой

**17) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:**

+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

**18) Окончательно, ответственность за защищенность данных в компьютерной сети несет:**

+ Владелец сети
- Администратор сети

- Пользователь сети

**19) Политика безопасности в системе (сети) – это комплекс:**

+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

**20) Наиболее важным при реализации защитных мер политики безопасности является:**

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций

**7.2.4Примерныйпереченьвопросовдляподготовкикзачету**

Непредусмотреноучебнымпланом

**7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач**

1. Общие понятия и классификация систем автоматического регулирования систем автоматического регулирования (САР). Примеры САР.
2. Статические характеристики *звеньев* САР. Способы линеаризации статической характеристики непрерывных САР (метод касательной, разложение в ряд Тейлора).
3. Динамические характеристики *звеньев* непрерывных САР. Входные импульсы. Весовая и переходная функции.
4. Уравнение переходного процесса и его связь с передаточной функцией *звена*. Пример.
5. Частотные характеристик *звена* (аналитический вид АЧХ, ФЧХ, АФЧХ, ЛАЧХ и ЛФЧХ).
6. Передаточные функции *систем*. Способы расчёта общей передаточной функции (расчётные формулы для последовательно/параллельно соединённых звеньев и для звеньев охваченных обратной связью). Пример.
7. Частотные характеристики *систем*. Пример формирования ЛАЧХ.
8. Передаточная функция замкнутых САР. Частотные характеристики замкнутых САР.
9. Переменные состояния динамической системы. Дифференциальные уравнения состояния.
10. Модели систем в переменных состояния в виде сигнального графа.
11. Определение устойчивости систем (по А.М. Ляпунову). Корневой *метод* оценки устойчивости непрерывных систем.
12. Критерии устойчивости Гурвица и Михайлова.
13. Критерии устойчивости Райса и Найквиста. Метод D-разбиения.
14. Метод трапеций. Качество регулирования. Быстродействие. Перерегулирование. Характер переходного процесса.

15. Синтез САР. Интегральный критерий работоспособности САР (построение ЛАЧХ и ЛФЧХ и определение запасов по амплитуде и фазе). Способы коррекции САР.

16. Виды регуляторов. П, ПИ и ПИД-регуляторы.

17. Разомкнутые и замкнутые цифровые САР. Блок схема цифрового компьютера.

18. Квантование сигнала по времени и по уровню. Теорема Котельникова-Шеннона (без доказательства).

19. Линейные законы цифрового управления (скользящее среднее, авторегрессионный процесс, авторегрессионный процесс со скользящим средним). Понятие разностного уравнения.

20. Операторные модели. Операторы прямого и обратного сдвига.

21. Восстановление непрерывных сигналов. Понятие экстраполятора. Фиксатор.

22. Линейные дискретные системы. z-преобразование. ξ-преобразование. Свойства z-преобразование (линейность, начальное и конечное значение, обратный сдвиг, сдвиг вперед, свёртка).

23. Импульсная характеристика линейной стационарной дискретной системы. Дискретная передаточная функция. Нули и полюса.

24. Типовые переходные процессы в дискретных системах. Модели в пространстве состояний.

25. Устойчивость линейных дискретных систем. Общие определения.

26. Алгебраические критерии устойчивости. Гурвица-Рауса, Джури.

27. Критерий Михайлова. Критерий Найквиста.

28. Термины и определения вариационного исчисления: функционал, вариация функционала, вариационная производная.

29. Постановка задачи вариационного исчисления. Задачи Лагранжа, Больца и Майера. Формула Эйлера.

30. Принцип максимума Понтрягина для решения задачи оптимального управления: сопряжённая система, условия трансверсальности, гамильтониан, краевая задача.

**7.2.6.Методикавыставленияоценкиприпроведениипромежуточной аттестации**

*(Например:Экзаменпроводитсяпотест-билетам,каждыйизкоторыхсодержит10вопросовизадачу.Каждыйправильныйответнавопросвтестеоценивается1баллом,задачаоценивается в10баллов(5балловверноерешениеи5балловзаверныйответ).Максимальноеколичестванабранныхбаллов–20.*

*1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабралменее6баллов.*

*2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабрало*

*т6до10баллов*

*3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15баллов.*

*4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.)*

**7.2.7Паспортоценочныхматериалов**

| №п/п | Контролируемыеразделы(темы) дисциплины | Кодконтролируемойкомпетенции | Наименованиеоценочногосредства |
|---|---|---|---|
| 1 | основные принципы построения защищенных распределенных компьютерных систем; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы | ПК-2, ПК-12, ПК- 15 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту…. |
| 2 | уметь формализовать задачу управления безопасностью информационных систем; анализировать защищенность компьютерных систем | ПК-12, ПК-15 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту…. |
| 3 | знать принципы построения СУИБ и, в её рамках, разработки процессов управления ИБ | ПК-12, ПК-15 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту…. |
| 4 | уметь анализировать состояние ИБ на предприятии в динамике с целью разработки требований к разрабатываемым процессам управления ИБ | ПК-2, ПК-12, ПК- 15 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту…. |
| 5 | владеть навыками выявления и устранения уязвимостей компьютерной сети; - навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем | ПК-2, ПК-12, ПК- 15 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту…. |
| 6 | знать основные понятия и последовательность этапов решения задачи управления необходимых для совершенствования системы управления информационной безопасностью компьютерной системы | ПК-2, ПК-12, ПК- 15 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту…. |

**7.3.Методическиематериалы,определяющиепроцедурыоценивания знаний,умений,навыкови(или)опытадеятельности**

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменатором,ивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведении промежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Защитакурсовойработы,курсовогопроектаилиотчетаповсемвидампрактикосуществляетсясогласнотребованиям,предъявляемымкработе,описаннымвметодическихматериалах.Примерноевремязащитынаодногостудентасоставляет20мин.

## 8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

**8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины**

Основная литература

1. Основы управления информационной безопасностью : Учеб.пособие / А. П. Курило. - М. : Горячая линия -Телеком, 2012. - 244 с. : ил . - (Вопросы управления информационной безопасностью. Кн. 1). - ISBN 978-5-9912-0271-8 : 300-00.

2.Методическое обеспечение оценки и регулирования рисков распределенных информационных систем : Учеб.пособие / Г. А. Остапенко [и др.]. - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2011. - 178 с. - 182-77; 250 экз.

3.Эпидемии в телекоммуникационных сетях [Текст] / Остапенко Александр Григорьевич [и др.] ; под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 282 с. : ил. - (Теория сетевых войн. № 1). - Библиогр.: с. 231-245 (244 назв.). - ISBN 978-5-9912-0682-2 : 736-00.

Дополнительная литература

1. Рыбак Л.А. Теория автоматического управления. Часть I. Непрерывные системы [Электронный ресурс]: учебное пособие/ Рыбак Л.А.— Электрон.текстовые данные.— Белгород: Белгородский государственный

технологический университет им. В.Г. Шухова, ЭБС АСВ, 2012.— 121 с.— Режим доступа: http://www.iprbookshop.ru/28400.html.— ЭБС «IPRbooks».

**2.** Эпидемии в телекоммуникационных сетях [Текст] / Остапенко Александр Григорьевич [и др.] ; под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 282 с. : ил. - (Теория сетевых войн. № 1). - Библиогр.: с. 231-245 (244 назв.). - ISBN 978-5-9912-0682-2 : 736-00.

3.Милославская Н.Г.Управление инцидентами информационной безопасности и непрерывного бизнеса : Учеб.пособие / Н. Г. Милославская, М. Ю. Сенаторов. - М. : Горячая линия -Телеком, 2012. - 214 с. : ил . - (Вопросы управления информационной безопасностью. Кн. 3). - ISBN 978-5-9912-0274-9 : 300-00.

**8.2Переченьинформационныхтехнологий,используемыхприосуществлениииобразовательногопроцессаподисциплине,включаяпереченьлицензионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:**

http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
https://marsohod.org/howtostart/marsohod2
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru
http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБСIPRbooks)

## 9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

## 10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Теорияуправленияинформационнойбезопасностьюраспределённыхкомпьютерныхсистем»читаютсялекции,проводятсяпрактическиезанятия,выполняетсякурсовойпроект.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяналиболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражениявучебнойлитературе.

Практическиезанятиянаправленынаприобретениепрактическихнавыков

:

- расчёта динамических и частотных характеристик САР;
- анализа и синтеза САР методом корневого годографа;
-описания систем в пространстве состояний;
- исследования устойчивости САР;
- синтеза оптимального управления с полной обратной связью

Занятияпроводятсяпутемрешенияконкретныхзадачваудитории.

Методикавыполнениякурсовогопроектаизложенавучебно-методическомпособии.Выполнятьэтапыкурсовогопроектадолжнысвоевременноивустановленныесроки.

Контрольусвоенияматериаладисциплиныпроизводитсяпроверкойкурсовогопроекта,защитойкурсовогопроекта.

| Видучебныхзанятий | Деятельностьстудента |
|---|---|
| Лекция | Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии. |
| Практическое занятие | Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму. |
| Самостоятельнаяработа | Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие:<br>- работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций;<br>- выполнение домашних заданий и расчетов;<br>- работа над темами для самостоятельного изучения;<br>- участие в работе студенческих научных конференций, олимпиад;<br>- подготовка к промежуточнойаттестации. |
| Подготовка к промежуточнойаттестации | Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом с оценкой, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала. |