**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ Гусев П.Ю.

«31» августа 2021 г.

# РАБОЧАЯ ПРОГРАММА

дисциплины

«Теория управления информационной безопасностью компьютерных систем (связь, информационные и коммуникационные технологии)»

**Специальность** 10.05.01 Компьютерная безопасность

**Специализация** специализация № 4 "Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)"

**Квалификация выпускника** специалист по защите информации

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

**Форма обучения** очная

**Год начала подготовки** 2021

Автор программы _____ /Разинкин К.А./

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

Руководитель ОПОП _____ / Остапенко А.Г./

Воронеж 2021

## 1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

**1.1. Целью дисциплины** 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. Задачи освоения дисциплины**

- 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. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Теория управления информационной безопасностью компьютерных систем (связь, информационные и коммуникационные технологии)» относится к дисциплинам обязательной части блока Б1.

## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Теория управления информационной безопасностью компьютерных систем (связь, информационные и коммуникационные технологии)» направлен на формирование следующих компетенций:

ОПК-8 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

ОПК-4.1 - Способен организовывать защиту информации в компьютерных системах и сетях (связь, информационные и коммуникационные технологии)

| Компетенция | Результаты обучения, характеризующие сформированность компетенции |
|---|---|
| ОПК-8 | знает основные формы, методы и приемы научного исследования при формализации математического обеспечения анализа и синтеза при проведении разработок в области обеспечения безопасности компьютерных систем и сетей |
| | уметь определить математический аппарат, необходимый для решения задачи управления в рамках динамической системы управления |

| | |
|---|---|
| | безопасностью компьютерной системы и применять критерии и методики оценки её работоспособности систем |
| | владеть навыками использования современных критериев и стандартов для анализа безопасности распределенных компьютерных систем, проведения анализа рисков и администрирования безопасности распределенных компьютерных систем |
| ОПК-4.1 | знать цели и задачи управления информационной безопасностью компьютерных систем (связь, информационные и коммуникационные технологии) |
| | уметь умеет применять методики организации защиты информации использовать средства защиты информации в компьютерных системах и сетях |

## 4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Теория управления информационной безопасностью компьютерных систем (связь, информационные и коммуникационные технологии)» составляет 6 з.е.

Распределение трудоемкости дисциплины по видам занятий

**очная форма обучения**

| Виды учебной работы | Всего часов | Семестры | |
|---|---|---|---|
| | | 5 | 6 |
| **Аудиторные занятия (всего)** | 108 | 54 | 54 |
| В том числе: | | | |
| Лекции | 72 | 36 | 36 |
| Лабораторные работы (ЛР) | 36 | 18 | 18 |
| **Самостоятельная работа** | 36 | 18 | 18 |
| Часы на контроль | 72 | 36 | 36 |
| Виды промежуточной аттестации - экзамен | + | + | + |
| Общая трудоемкость:<br>академические часы<br>зач.ед. | <br>216<br>6 | <br>108<br>3 | <br>108<br>3 |

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

**очная форма обучения**

| № п/п | Наименование темы | Содержание раздела | Лекц | Лаб. зан. | СРС | Всего, час |
|---|---|---|---|---|---|---|
| 1 | Введение в теорию автоматического управления. Не-прерывные 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 | 12 | 6 | 6 | 24 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 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. 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 авто-матического управления. D–разбиение. Понятие качества регулирования. Прямые показатели качества: перерегулирование, быстро- действие, 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 системы управления | Цифровые законы управления. Описание работы цифровой части. Линейные законы управления. Операторные модели. Восста- новление непрерывных сигналов. Понятие экстраполятора. Анализ последовательностей Z и ζ -преобразование. Вычисление изобра-жений. Свойства z-преобразования. Восстановление оригинала. Линейные дискретные системы. Импульсная характеристика. Дискретная передаточная функция. Нули и по- люса. Типовые переходные процессы. Модели в пространстве состояний. Физическая реализуемость. Устойчивость. Устойчивость по А.М. Ляпунову. Устойчивость линейных си- стем. Алгебраические критерии | 12 | 6 | 6 | 24 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | устойчивости. Критерий Михайлова. Критерий Найквиста. Одноконтурная дискретная система. Структурная схема. | | | | |
| 3 | Оптимальное управление | 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 терминально- го 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 задач с помощью метода Беллмана: задача о распределении ресурсов, о замене оборудования и т.д. | 12 | 6 | 6 | 24 |
| 4 | Основы управления 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 | 12 | 6 | 6 | 24 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 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. **Active Directory.** Управление учетными записями. Доверительные отноше- ния. Инструменты администрирования. Групповая политика. Расширяемость. Разделение физической сети. **OpenLDAP.** Откры- тая реализация LDAP. История появления OpenLDAP. Основные компоненты OpenLDAP. | | | | |
| 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. Об- щее 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. Уязви- мости и методы оценки уязвимостей. Подходы к оценке риска ИБ. | 12 | 6 | 6 | 24 |
| 6 | Администрирование средств безопасно сти | Управление ключами (генерация и распределение). Управление шифрованием (установка и синхронизация криптографических параметров). Администрирование управления доступом (распределение информации, необходимой для управления - паролей, списков до- ступа и т.п.). Управление аутентификацией (распределение информации, необходимой 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 | 12 | 6 | 6 | 24 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | нотариальных службах, администрирование этих служб). | | | | |
| | | **Итого** | **72** | **36** | **36** | **144** |

### 5.2 Перечень лабораторных работ

- расчёт динамических и частотных характеристик САР;
- анализ и синтез САР методом корневого годографа;
- описание систем в пространстве состояний;
- исследование устойчивости САР;
- синтез оптимального управления с полной обратной связью.
- фильтр Калмана.

## 6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

## 7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

### 7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

#### 7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

| Компетенция | Результаты обучения, характеризующие сформированность компетенции | Критерии оценивания | Аттестован | Не аттестован |
|---|---|---|---|---|
| ОПК-8 | знает основные формы, методы и приемы научного исследования при формализации математического обеспечения анализа и синтеза при проведении разработок в области обеспечения безопасности компьютерных систем и сетей | знание основных форм, методов и приемов научного исследования при формализации математического обеспечения анализа и синтеза при проведении разработок в области обеспечения безопасности компьютерных систем и сетей | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | уметь определить математический аппарат, необходимый для | умение определить математический аппарат, необходимый для решения задачи управления в рамках | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

| | | | | |
|---|---|---|---|---|
| | решения задачи управления в рамках динамической системы управления безопасностью компьютерной системы и применять критерии и методики оценки её работоспособности систем | динамической системы управления безопасностью компьютерной системы и применять критерии и методики оценки её работоспособности систем | | |
| | владеть навыками использования современных критериев и стандартов для анализа безопасности распределенных компьютерных систем, проведения анализа рисков и администрирования безопасности распределенных компьютерных систем | владение навыками использования современных критериев и стандартов для анализа безопасности распределенных компьютерных систем, проведения анализа рисков и администрирования безопасности распределенных компьютерных систем | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ОПК-4.1 | знать цели и задачи управления информационной безопасностью компьютерных систем (связь, информационные и коммуникационные технологии) | знание целей и задач управления информационной безопасностью компьютерных систем (связь, информационные и коммуникационные технологии) | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | уметь умеет применять методики организации защиты информации использовать средства защиты информации в компьютерных системах и сетях | умение применять методики организации защиты информации использовать средства защиты информации в компьютерных системах и сетях | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

### 7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 5, 6 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

| **Компе-тенция** | **Результаты обучения, характеризующие сформированность компетенции** | **Критерии оценивания** | **Отлично** | **Хорошо** | **Удовл.** | **Неудовл.** |
|---|---|---|---|---|---|---|
| ОПК-8 | знает основные формы, методы и приемы научного исследования при формализации математического обеспечения анализа и синтеза при проведении разработок в области обеспечения безопасности компьютерных систем и сетей | Тест | Выполнение теста на 90-100% | Выполнение теста на 80-90% | Выполнение теста на 70-80% | В тесте менее 70% правильных ответов |
| | уметь определить математический аппарат, необходимый для решения задачи управления в рамках динамической системы управления безопасностью компьютерной системы и применять критерии и методики оценки её работоспособности систем | Решение стандартных практических задач | 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 | Задачи не решены |
| | владеть навыками использования современных критериев и стандартов для анализа | 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 | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены |

| | | | | | | |
|---|---|---|---|---|---|---|
| | безопасности распределенных компьютерных систем, проведения анализа рисков и администрирования безопасности распределенных компьютерных систем | | | задачах | | |
| ОПК-4.1 | знать цели и задачи управления информационной безопасностью компьютерных систем (связь, информационные и коммуникационные технологии) | Тест | Выполнение теста на 90-100% | Выполнение теста на 80-90% | Выполнение теста на 70-80% | В тесте менее 70% правильных ответов |
| | уметь умеет применять методики организации защиты информации использовать средства защиты информации в компьютерных системах и сетях | Решение стандартных практических задач | 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 | Задачи не решены |

**7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)**

**7.2.1 Примерный перечень заданий для подготовки к тестированию**

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 ивозмущающего 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 ивозмущающего воздействий;

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

C) на вход автоматического регулятора поступает разность задающеговоздействия 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 ивозмущающего воздействий;**

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

C) на вход автоматического регулятора поступает разность задающеговоздействия 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, КОТОРАЯХАРАКТЕРИЗУЕТСЯПРОИЗВОЛЬНЫМ 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 КОТОРОЙЗАДАЮЩЕЕ 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 посто**янно;

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 изменяетсяпо случайному закону.

11. НЕЛИНЕЙНОЙ НАЗЫВАЕТСЯ ТАКАЯ СИСТЕМА АВТОМАТИЧЕСКОГО РЕГУЛИРОВАНИЯ:

A) которая обладает способностью приспосабливаться к

измененииювнешних условий;

B) все параметры которой изменяются во времени;

C) которая описывается линейными дифференциальными уравнениямилюбого 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 измененииювнешних условий;

B) все параметры которой изменяются во времени;

C) которая описывается линейными дифференциальными уравнениямилюбого порядка;

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

E) в состав которой входит хотя бы одно звено, описываемое уравнениямивида 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 уравнениямилюбого 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

### 7.2.2 Примерный перечень заданий для решения стандартных задач

| | |
|---|---|
| **ПК-2 способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информациив компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований** | |
| 1. | Предполагает ли экспертно-документальный метод проверки использование средств измерений?<br>а) да б) **нет** |
| 2. | Проверка объекта информатизации в целях выявления и изъятия воз-можно внедренных закладочных устройств - это:<br>а) специальные исследования; б) оценка защищенности;<br>в) **специальная проверка**. г) контроль эффективности |
| 3. | Укажите методы оценки эффективности средств защиты от несанкционированного доступа:<br>**а) метод экспертно-документального контроля;**<br>**б) метод тестирования функций, реализованных средствами защиты информации от несанкционированного доступа;**<br>в) инструментальный метод<br>г) инструментально-расчетный метод |
| 4. | В каких случаях проводится специальная проверка технических средств,<br>входящих в состав объекта информатизации, обрабатывающего информацию, не содержащую сведения, составляющие государственную тайну?<br>а) по требованию органа по аттестации;<br>б) по решению аттестационной комиссии;<br>в) **по решению владельца объекта информатизации;**<br>г) при отрицательных выводах «Заключения по результатам аттестационных испытаний». |

| | |
|---|---|
| 5. | Выберите данные, указываемые в Предписании на эксплуатацию технических средств?<br>а) **состав основных и вспомогательных технических средств и систем;**<br>**б) перечень средств защиты информации;**<br>**в) расположение объекта информатизации относительно границ контроли**<br>**руемой зоны;**<br>г) таблицы результатов специальных исследований и расчетов нормативных показателей;<br>д) лист регистрации изменений;<br>е) схема сетиэлектропитания и заземления |
| 6. | К правовым методам, обеспечивающим информационную безопасность,<br>относятся…<br>а) разработка аппаратных средств обеспечения правовых данных;<br>б) разработка и установка во всех компьютерных правовых сетях журналов учета действий;<br>**в) разработка и конкретизация правовых нормативных актовобеспечения безопасности** |
| 7. | Основными источниками угроз информационной безопасности являются<br>все указанное в списке ...<br>а) хищение жестких дисков, подключение к сети, инсайдерство;<br>**б) перехват данных, хищение данных, изменение архитектуры системы;**<br>в) хищение данных, подкуп системных администраторов, нарушениерегламента работы |
| 8. | Виды информационной безопасности:<br>а) **персональная, корпоративная, государственная;**<br>б**)** клиентская, серверная, сетевая;<br>в) локальная, глобальная, смешанная |
| 9. | **Цели информационной безопасности – своевременное обнаружение,предупреждение:**<br>а) **несанкционированного доступа, воздействия в сети;**<br>б) инсайдерства в организации;<br>в) чрезвычайных ситуаций |
| 10. | **Основные объекты информационной безопасности:**<br>а) **компьютерные сети, базы данных**<br>б) информационные системы, психологическое состояние пользователей<br>в) бизнес-ориентированные, коммерческие системы |

| | |
|---|---|
| 11. | **Основными рисками информационной безопасности являются:**<br>а) искажение, уменьшение объема, перекодировка информации;<br>б) техническое вмешательство, выведение из строя оборудования сети<br>в) **потеря, искажение, утечка информации** |
| 12. | **К основным принципам обеспечения информационной безопасностиотносится**<br>а) **экономической эффективности системы безопасности**;<br>б) многоплатформенной реализации системы;<br>в) усиления защищенности всех звеньев системы. |
| 13. | **Основными субъектами информационной безопасности являются:**<br>а) руководители, менеджеры, администраторы компаний;<br>б) **органы права, государства, бизнеса;**<br>в) сетевые базы данных, фаерволлы |
| 14. | **К основным функциям системы безопасности можно отнести всеперечисленное:**<br>а) **установление регламента, аудит системы, выявление рисков**;<br>б) установка новых офисных приложений, смена хостинг-компании;<br>в) внедрение аутентификации, проверки контактных данных пользова-телей |
| 15. | Принципом информационной безопасности является принцип недопущения<br>а) **неоправданных ограничений при работе в сети (системе);**<br>б) рисков безопасности сети, системы<br>в) презумпции секретности |
| 16. | **Принципом политики информационной безопасности являетсяпринцип:**<br>а) **невозможности миновать защитные средства сети (системы)**;<br>б) усиления основного звена сети, системы<br>в) полного блокирования доступа при риск-ситуациях |
| 17. | **Принципом политики информационной безопасности являетсяпринцип:**<br>а) **усиления защищенности самого незащищенного звена сети (системы)**;<br>б) перехода в безопасное состояние работы сети, системы;<br>в) полного доступа пользователей ко всем ресурсам сети, системы |
| 18. | **Принципом политики информационной безопасности являетсяпринцип:**<br>**а) разделения доступа (обязанностей, привилегий) клиентам сети** |

| | |
|---|---|
| | **(системы);**<br>б) одноуровневой защиты сети, системы;<br>г) совместимых, однотипных программно-технических средств сети,системы |
| 19. | **К основным типам средств воздействия на компьютерную сеть относится:**<br>а) компьютерный сбой;<br>б) **логические закладки («мины»)**;<br>г) аварийное отключение питания |
| 20. | **Угроза информационной системе (компьютерной сети) – это:**<br>а) **вероятное событие**;<br>б) детерминированное (всегда определенное) событие;<br>в) событие, происходящее периодически |
| 21. | **Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:**<br>а) регламентированной;<br>б) правовой;<br>**в) защищаемой** |
| 22. | **Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:**<br>а) **программные, технические, организационные, технологические**;<br>б) серверные, клиентские, спутниковые, наземные;<br>в) личные, корпоративные, социальные, национальные |
| 23. | **Окончательно, ответственность за защищенность данных в компьютерной сети несет:**<br>а) **владелец сети;**<br>б) администратор сети;<br>в) пользователь сети |
| 24. | **Политика безопасности в системе (сети) – это комплекс:**<br>а) **руководств, требований обеспечения необходимого уровня безопасности**;<br>б) инструкций, алгоритмов поведения пользователя в сети;<br>в) нормы информационного права, соблюдаемые в сети |
| 25. | **Наиболее важным при реализации защитных мер политики безопасности является:**<br>а) аудит, анализ затрат на проведение защитных мер;<br>б) аудит, анализ безопасности<br>**в) аудит, анализ уязвимостей, риск-ситуаций** |

| **ПК-12 — способностью проводить инструментальный мониторинг защищенности компьютерных систем** | |
|---|---|
| 1. | С какой целью при разработке и реализации политики безопасности используются метрики?<br>а) для определения рамок, в которых осуществляются мероприятия по обеспечению безопасности информации, и задаются критерии оценкиполученных результатов;<br>б) для замеров уровней безопасности;<br>в) **с целью определения параметров защищенности системы, чтопозволяет соотнести сделанные затраты и полученный эффект** |
| 2. | Может организация разрабатывать и применять собственные (корпоративные) стандарты безопасности?<br>а) нет, это недопустимо;<br>**б) да, это не запрещено;**<br>в) это требует множественных согласований, поэтому разработка своихстандартов не распространена |
| 3. | В каких целях осуществляется анализ рисков?<br>а) в целях соблюдения требований об обязательной отчетности учреждения, его проведение формально необходимо;<br>**б) в целях установления и поддержания эффективного управлениясистемой защиты;**<br>в) в целях укрепления имиджевой политики учреждения; |
| 4. | В каких целях разрабатываются методы реагирования в случае инцидентов?<br>а) **в целях обеспечения эффективных мер защиты;**<br>б) в целях обеспечения расширения функционала сотрудников учреждения;<br>в) **в целях обеспечения скорейшего восстановления работоспособности системы в случае инцидентов** |
| 5. | Решению каких из перечисленных задач способствует разработка стратегического плана построения системы безопасности?<br>а) **распределение бюджетов и ресурсов по приоритетам**;<br>**б) эффективный выбор продуктов и разработка стратегий их внедрения**;<br>в) получение кредитов на развитие ИБ в кредитных учреждениях на льготных основаниях. |

| | |
|---|---|
| 6. | Какова связь анализа рисков с другими компонентами модели информационной безопасности?<br>**а) на базе полученных результатов по оценке рисков осуществляется анализ состояния системы и разрабатывается план построениясистемы защиты сети;**<br>б) анализ рисков увязан с процедурами анализа рисков;<br>в) анализ не увязывается с другими компонентами системы |
| 7. | Что из перечисленного не входит в систему мер по ограничению физического доступа?<br>а) защита помещений, контроль доступа, видеонаблюдение;<br>б) **защита коллатеральных сетей, используемых сотрудниками**;<br>в)защита мобильных устройств, используемых сотрудниками в служебных целях |
| 8. | Какие из перечисленных средств применяются для защиты сети в "точках входа"?<br>**а) средства антивирусной защиты для шлюзов безопасности**;<br>**б) межсетевые экраны (firewall)** ;<br>**в) системы обнаружения вторжений** |
| 9. | На что нацелен уровень защиты внутренней сети?<br>а) на защиту сети от спама, поступающего на почтовые ящики сотрудников;<br>б) на скрининг деятельности сотрудников по посещению ими web-узлов;<br>**в) на обеспечение безопасности передаваемого внутри сети трафикаи сетевой инфраструктуры** |
| 10. | Каким аспектам рекомендуется уделять первоочередное внимание при защите узлов?<br>а) функциональности узлов;<br>**б) защите на уровне операционной системы**<br>в) защите серверов и рабочих станций |
| 11. | За какие из перечисленных аспектов "отвечает" уровень защиты приложений?<br>**а) защита от атак, направленных на нарушение логики обработки данных базами данных;**<br>**б) защита от атак, направленных на конкретные приложения - почтовые серверы, web-серверы, серверы базданных;**<br>**в) защита от вирусных атак** |
| 12. | Является ли шифрование данных при их хранении и передаче адекватной<br>мерой защиты?<br>**а) нет;** |

| | |
|---|---|
| | **б)** да**;**<br>**в)** лишь частично |
| 13. | К какому состоянию зрелости управления рисками безопасности согласно методики фирмы Microsoft относится уровень, когда процесс управления рисками глубоко изучен сотрудниками и в значительнойстепени автоматизирован?<br>а) управляемый;<br>б) **оптимизированный** |
| 14. | К какому состоянию зрелости управления рисками безопасности, согласно методики фирмы Microsoft, относится уровень, когда процесс документирован не полностью, но управление рисками является всеобъемлющим и руководство вовлечено в управление рисками?<br>а)оптимизированный;<br>б) **повторяемый;**<br>в) узкоспециализированный |
| 15. | К какому состоянию зрелости управления рисками безопасности согласно методики фирмы Microsoft относится уровень, когда политики ипроцессы в организации не документированы, процессы не являются полностью повторяемыми?<br>а)оптимизированный;<br>б) повторяемый;<br>в) **узкоспециализированный** |
| 16. | К какому состоянию зрелости управления рисками безопасности согласно методики фирмы Microsoft относится уровень, когда принято |
| | формальное решение об интенсивном внедрении управления рисками,разработан базовый процесс и внедряется управление рисками?<br>а) **наличие определенного процесса**;<br>б) повторяемый;<br>в) оптимизированный |
| 17. | Что контролирует уровень защиты узлов?<br>а) **парирование атак на отдельный узел сети. Может учитываться функциональность узла и отдельно рассматриваться защита серверов и рабочих станций**;<br>б) защиту обрабатывающихся и хранящихся в системе данных от несанкционированного доступа и других угроз;<br>в) безопасность передаваемого внутри сети трафика и сетевой инфраструктуры |
| 18. | Относится ли модификация приложений компьютерными вирусами к разряду SQL-инъекций?<br>**а) да**<br>б) нет |

| | |
|---|---|
| | в) нет, но такая классификация модификаций возможна впринципе |
| 19. | Характерно использование внутри сети средств, применимых для защиты периметра**?**<br>**а) да, например, межсетевые экраны, в том числе иперсональные (устанавливаемые на защищаемый компьютер)**;<br>б) нет, внутри сети средства, характерные для защиты периметра, такие как межсетевыве экраны, не применяются;<br>в) нет, внутри сети нет необходимости применения каких-либо барьерных механизмов |
| 20. | Может ли защита серверов осуществляться отдельно от защиты рабочих<br>станций?<br>**а) да, это возможно**;<br>б) нет, это не практикуется;<br>в) если сетьнадежно защищена извне, отдельной защиты для станций организовывать необходимости нет |
| 21. | Какие из перечисленных контрмер можно назвать в качестве примера, характерного для уровня защиты данных?<br>**а) разграничение доступа к данным средствами файловой системы;**<br>**б) шифрование данных при хранении и передаче;**<br>в) кодификация информации |
| 22. | Является ли возможным в процессе идентификации рисков определить цели потенциального нарушителя и уровни защиты, на которых можноему противостоять?<br>а)нет<br>б**) да**<br>в) нет, но такая попытка может дать некий эффект |
| 23. | Как можно проверить информацию о соответствии имен компьютеров IP-адресам в OS Windows?<br>а) **при обращении к утилите командной строки nslookup**<br>**б) при обращении к административной оснастке "DNS"**<br>в) при обращении к функции autoexec |
| 24. | Какие средства можно использовать для получения данных о системе, если в информационной системе используются домены Windows? |

| | |
|---|---|
| | а) средства синхронизации данных, реализованные в виде консоли администрирования<br>**б) средства администрирования, реализованные в виде оснасток консоли администрирования (Microsoft management console - mmc)**<br>в**)** средства администрирования, реализованные в виде консоли журналыи оповещения производительности (Microsoft management console -mmc). |
| 25. | Какие сведения содержит оснастка "Active Directory Users and Computers"?<br>а) о сетевой идентификации<br>**б) о членстве пользователя в доменных группах**<br>**в)** реестр сведений о членстве пользователей в сетевых профессиональных союзах и группах |
| ПК-15 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы | |
| 1. | Управление без непосредственного участия человека называется:<br>**а) дистанционным;**<br>в) автоматизированным;<br>с) автоматическим;<br>d) телемеханическим;<br>е) централизованным. |
| 2. | Управление с частичным участием человека называется:<br>а) дистанционным;<br>**в) автоматизированным;**<br>с) автоматическим;<br>d) телемеханическим;<br>е) централизованным |
| 3. | Управление без участия человека называется:<br>а) дистанционным;<br>в) автоматизированным;<br>**с) автоматическим;**<br>d)телемеханическим;<br>е)централизованным |

| | |
|---|---|
| 4. | Замкнутой системой по отклонению называется такая система, в которой:<br>а) на вход автоматического регулятора поступает сумма задающего ивозмущающего воздействий;<br>в) на вход автоматического регулятора поступает сумма нескольких задающих воздействий с разными знаками;<br>**с) на вход автоматического регулятора поступает разность задающего воздействия и выходной величины;**<br>d) на вход автоматического регулятора поступает сумма задающего,возмущающего воздействий и выходной величины;<br>е) на вход автоматического регулятора поступает задающее воздействие |
| 5. | Разомкнутой системой первого рода называется такая система, в которой:<br>а) на вход автоматического регулятора поступает сумма задающего ивозмущающего воздействий;<br>в) на вход автоматического регулятора поступает сумма нескольких задающих воздействий с разными знаками;<br>с) на вход автоматического регулятора поступает разность задающего воздействия и выходной величины;<br>d) на вход автоматического регулятора поступает сумма задающего, возмущающего воздействий и выходной величины;<br>**е) на вход автоматического регулятора поступает задающее воздействие** |
| 6. | Разомкнутой системой второго рода называется такая система, в которой:<br>**а) на вход автоматического регулятора поступает сумма задающегои возмущающего воздействий;**<br>в) на вход автоматического регулятора поступает сумма нескольких задающих воздействий с разными знаками;<br>с) на вход автоматического регулятора поступает разность задающего воздействия и выходной величины;<br>d) на вход автоматического регулятора поступает сумма задающего,возмущающего воздействий и выходной величины;<br>е) на вход автоматического регулятора поступает задающее воздействие. |
| 7. | Система автоматического регулирования, которая характеризуется произвольным законом изменения задающего воздействия во времени,называется:<br>**а) следящей;**<br>в) статической;<br>с) астатической;<br>d) программной;<br>е) системой стабилизации. |

| | |
|---|---|
| 8. | Система автоматического регулирования, в которой задающее воздействие постоянно во времени, называется:<br>а) следящей;<br>в)статической;<br>с)астатической;<br>d) программной;<br>**е) системой стабилизации** |
| 9. | Система автоматического регулирования, в которой задающее воздействие изменяется по заранее заданному закону, называется:<br>а) следящей;<br>в)статической;<br>с)астатической;<br>**d) программной;**<br>е) системой стабилизации |
| 10. | Системой стабилизации называется:<br>а) автоматическая система, в которой отсутствует обратная связь;<br>**в) автоматическая система, в которой задающее воздействие постоянно;**<br>с) автоматическая система, в которой задающее воздействие изменяетсяпо заранее заданному закону;<br>d) автоматическая система, на которую не воздействуют внешние возмущающие воздействия;<br>е) автоматическая система, в которой задающее воздействие изменяетсяпо случайному закону. |
| 11. | Нелинейной называется такая система автоматического регулирования:<br>а) которая обладает способностью приспосабливаться к измененииювнешних условий;<br>в) все параметры которой изменяются во времени;<br>с) которая описывается линейными дифференциальными уравнениямилюбого порядка;<br>d) в которой все звенья описываются уравнениями вида y=kx;<br>**е) в состав которой входит хотя бы одно звено, описываемое нелинейными уравнениями** |
| 12. | Импульсной называется такая система автоматического регулирования:<br>а) которая обладает способностью приспосабливаться к измененииювнешних условий;<br>в) все параметры которой изменяются во времени;<br>с) которая описывается линейными дифференциальными уравнениямилюбого порядка;<br>**d) в состав которой входит хотя бы одно импульсное звено;**<br>е) в состав которой входит хотя бы одно звено, описываемое уравнени-ями вида y=kx |

| | |
|---|---|
| 13. | Релейной называется такая система автоматического регулирования:<br>а) которая обладает способностью приспосабливаться к измененииювнешних условий;<br>**в) в состав которой входит хотя бы одно релейное звено;**<br>с) которая описывается линейными дифференциальными уравнениямилюбого порядка;<br>d) в состав которой входит хотя бы звено, описываемое уравнением видау=kx;<br>е) все параметры которой изменяются во времени |
| 14. | Системой прямого действия называется:<br>а) система, в которой выходная величина изменяется прямо пропорционально входной;<br>в) вычислительная система с управляющим компьютером;<br>с) трехвходовая система;<br>**d) система с регулятором без дополнительного источника энергии;**<br>е) система с регулятором использующим дополнительный источник энергии |
| 15. | Системой прямого действия называется:<br>а) система, в которой выходная величина изменяется прямо пропорционально входной;<br>в) вычислительная система с управляющим компьютером;<br>с) трехвходовая система;<br>**d) система с регулятором без дополнительного источника энергии;**<br>е) система с регулятором использующим дополнительный источникэнергии |
| 16. | Объектом регулирования называется:<br>а) устройство, совокупность устройств или часть устройства предназначенное для обеспечения заданных параметров качества процесса регулирования;<br>**в) устройство, совокупность устройств или часть устройства предназначенное для выполнения рабочей операции;**<br>с) устройство, совокупность устройств или часть устройства имеющеедве входные величины;<br>d) устройство, совокупность устройств или часть устройства выполняющее операцию сравнения входной и выходной координаты;<br>е) устройство, совокупность устройств или часть устройства обеспечивающее требуемые параметры качества технологического процесса |

**7.2.3 Примерный перечень заданий для решения прикладных задач**

| |
|---|
| **ПСК-3.1–способностью использовать современные критерии и стандартыдля анализа безопасности распределенных компьютерных** |

| |
|---|
| **систем** |
| NIDS называется так, потому что:<br>а) **располагается на одном компьютере и следит за трафиком в сегментесети**<br>б**)** располагается на нескольких компьютерах объединенных в сеть<br>в) отслеживает атаки на определенный узел |
| Какие типы систем обнаружения вторжения существуют?<br>а) **сетевые**<br>**б) узловые**<br>в)распределенные<br>г) локальные |
| Сколько существует основных типов датчиков HIDS?<br>а) 4<br>б) **5**<br>в) 3<br>г) 2 |
| Не существует следующего типа датчиков:<br>а) анализаторы журналов<br>б) датчики признаков<br>в) **анализаторы трафика**<br>г) анализаторы поведения приложений |
| Существуют датчики:<br>а) **анализаторы журналов**<br>**б) контроллеры целостности файлов** |
| в) анализаторы трафика<br>г) **анализаторы поведения приложений** |
| Датчик отслеживающий изменения журналов называется?<br>а) **анализатор журналов**<br>б) контроллер целостности файлов<br>в) анализатор поведения приложений |
| Датчик отслеживающий системные вызовы называется?<br>а) анализаторы журналов<br>б) **контроллеры целостности файлов**<br>в) анализатор системных вызовов |
| Датчик отслеживающий изменения файлов называется?<br>а) анализаторы журналов<br>б) контроллеры целостности файлов<br>в) анализаторы поведения приложений |

| |
|---|
| Отличие анализаторов системных вызовов от анализаторов журналов и датчиков признаков заключается в том, что:<br>а) **анализатор системных вызовов может предотвращать действия**<br>б) может выполнять функции двух других<br>в) хорошо подходит для отслеживания деятельности авторизированныхпользователей |
| К чему может привести неправильная настройка анализатора системных вызовов?<br>а) **блокировке легитимных приложений;**<br>б) ничего не произойдет<br>в) датчик не будет работать |
| Каким образом контроллеры целостности файлов отслеживают изменения?<br>а) сохраняют в своей базе копию файла<br>б) **сохраняют контрольную сумму файла**<br>**в) сохраняют цифровую подпись файла** |
| Принцип работы NIDS заключается в:<br>а) подключении ко всем системам и анализе их работы<br>б) **перехвате сетевого трафика и его анализе**<br>в) выполнении обоих вышеуказанных действий |
| На чем базируется работа NIDS?<br>а) **на наборе признаков атак**<br>б) на нечетком анализе трафика<br>в) на применении самообучающихся систем |
| Что произойдет если произойдет атака признак которой отсутствует в базе?<br>а) **атака не будет обнаружена**<br>б) атака будет обнаружена<br>в) это приведет к зависанию датчика |
| Сколько сетевых карт обычно используется в NIDS?<br>а) 1<br>б) 3<br>в) **2**<br>г) 4 |
| Куда подключаются сетевые карты NIDS?<br>а) **одна к наблюдаемой сети, другая к сети для отправки сигналов тревоги**<br>б) обе к наблюдаемой сети, причем одна карта находится в резерве<br>в) обе к наблюдаемой сети обе карты работают |

| |
|---|
| В чем особенность работы сетевой карты с помощью которой производится<br>наблюдение?<br>а) никаких особенностей нет, она работает как обычная<br>карта<br>б) **не имеет IP-адреса**<br>в) **отсутствует стек протоколов** |
| Какая система дешевле для использования в большой сети?<br>а)HIDS<br>**б)NIDS**<br>в) стоимость одинакова |
| Какие цели могут преследоваться при установке IDS?<br>а) **обнаружение атак**<br>б) **обнаружение нарушений политики**<br>в) повышение надежности<br>системы<br>г) **сбор доказательств** |
| Какие цели могут преследоваться при установке IDS?<br>а) повышение надежности системы;<br>б) **принуждение к использованию политик;**<br>в) **принуждениек следованию политикам соединений;**<br>**г) сбор доказательств** |
| Какие цели могут преследоваться при установке IDS?<br>а) **обнаружение атак**<br>**б) предотвращение атак**<br>**в) обнаружение нарушений политики**<br>г) повышение надежности системы |
| Что является объектом мониторинга при обнаружении атак с помощью HIDS?<br>а) весь трафик, поступающий на потенциально атакуемые<br>системы**б) неудачные попытки входа**<br>**в) попытки соединения**<br>**г) удачный вход с удаленных систем** |
| Что является объектом мониторинга при обнаружении атак с помощью NIDS?<br>а) **весь трафик, поступающий на потенциально атакуемые системы**<br>б) неудачные попытки входа<br>в)успешные HTTP-соединения<br>г) успешные FTP-соединения |
| Что является объектом мониторинга при сборе доказательств с помощью NIDS?<br>а) **содержимое всего трафика, формируемого на системе-цели или атакующей системе**<br>б) неудачные попытки входа<br>в) успешные |

| |
|---|
| HTTP-соединения<br>г) успешные<br>FTP-соединения |
| Какие пассивные действия можно предпринять при обнаружении атак?<br>а) **ведение журнала**<br>б) никаких действий<br>в) **ведение дополнительных**<br>**журналов**<br>**г) уведомление** |
| Какие активные действия можно предпринять при обнаружении атак?<br>а) ведение журнала<br>б) **никаких действий**<br>в) ведение дополнительных<br>журналов<br>г) уведомление |
| Какие активные действия можно предпринять при предотвращении атак?<br>а) ведение журнала;<br>**б) закрытие**<br>**соединения;**<br>**в) завершение**<br>**процесса;**<br>г) уведомление |
| Попытки идентификации систем, присутствующих в сети, с целью предотвратить обнаружение системы, с которой будет проводиться атака – это…<br>а) **скрытое сканирование**;<br>б**)** сканирование портов;<br>в) сканирование «троянских коней»;<br>г) сканирование уязвимостей |
| Данный тип сканирования может быть распознан только датчиком HIDS:<br>а) скрытое сканирование;<br>б**) отслеживание файлов**;<br>в**)** сканирование «троянских коней»;<br>г**)** сканирование уязвимостей |
| Данный тип сканирования осуществляемого хакерами, невозможно отличить<br>от сканирования, проводимого компаниями<br>**а)** скрытое сканирование;<br>б**)** отслеживание файлов;<br>в**)** сканирование «троянских коней»;<br>г**) сканирование уязвимостей** |
| **ПСК-3.5–способностью участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем** |

| |
|---|
| Согласно закону "О техническом регулировании", стандарт - это<br>**а) документ, в котором в целях добровольного многократного использования сформулированы характеристики продукции**<br>б) требование соблюдения единообразия технических и иных характеристик<br>в) изделие, характеристики которого считаются эталонными |
| Согласно закону "О техническом регулировании", стандартизация - это<br>**а)** деятельность по выработке единых требований к техническим и иным характеристикам продукции<br>**б) деятельность по установлению правил и характеристик в целях ихдобровольного многократного использования**<br>**в)** деятельность по установлению единообразия в сфере производства и иных<br>сферах |
| Согласно закону "О техническом регулировании", принципом стандартизации<br>является<br>а) приоритет национальных законодательных и технических актов<br>б) обеспечение конкурентоспособности российских товаров и услуг на мировом рынке<br>**в) применение международного стандарта как основы разработки национального стандарта** |
| В "Оранжевой книге" фигурируют понятия:<br>**а)** ядро безопасности;<br>**б)** периметр безопасности;<br>**в)** центр безопасности |
| В "Гармонизированных критериях Европейских стран" фигурируют понятия:<br>**а) цель**<br>**оценки б)**<br>система<br>оценки<br>**в) объект оценки** |
| В рекомендациях X.800 фигурируют понятия:<br>а) регулятор безопасности<br>**б) сервис безопасности**<br>**в) механизм безопасности** |
| "Общие критерии" содержат следующие основные виды требований безопас-<br>ности:<br>а) архитектурные требования<br>**б) функциональные**<br>**требования**<br>**в) требования доверия** |

| |
|---|
| Пользователями интерфейса безопасности GSS-API являются:<br>**а) коммуникационные протоколы**<br>**б)** администраторы безопасности<br>**в) программные системы** |
| В стандарте BS 7799 разъясняются следующие понятия и процедуры:<br>**а)** безопасность интерфейсов<br>**б) безопасность персонала**<br>**в) физическая безопасность** |
| Стандарты и спецификации подразделяются в курсе на<br>**а) оценочные стандарты**<br>**б) технические спецификации**<br>**в)** нормативные спецификации |
| Изучение стандартов и спецификаций необходимо, поскольку<br>а) создаются условия для разработки безопасных систем<br>**б) они являются формой накопления знаний с целью многократного использования**<br>в) невыполнение их требований преследуется по закону |
| Согласно закону "О техническом регулировании", стандарты могут содержать требования к<br>**а)** структуре документации<br>**б)терминологии**<br>**и**<br>**в)**<br>**символике** |
| Спецификация IPsec затрагивает вопросы<br>**а)** доступности<br>**б)конфиденциальност**<br>**и**<br>**в) целостности** |
| Спецификация TLS близка к |
| **а)SS**<br>**L**<br>**б)**SS<br>H<br>**в)**D<br>NS<br>Рекомендации X.509 регламентируют формат<br>**а)** сертификата безопасности |

**б) сертификата открытого ключа**
**в)** сертификата директории

**7.2.4 Примерный перечень вопросов для подготовки к зачету**

Не предусмотрено учебным планом

**7.2.5 Примерный перечень заданий для решения прикладных задач**

1. Дайте определения управления доступом (логическим), правил разграничения доступа, объекта и субъекта доступа.
2. Каковы назначение и основные достоинства унифицированных систем управления идентификацией?
3. Каковы назначение и основные достоинства унифицированных систем управления идентификацией?
4. На основе, каких документов, процедур и средств осуществляется управление доступом пользователей к активам организации?
5. Как должны назначаться и использоваться привилегированные права доступа?
6. Руководствуясь какими рекомендациями пользователи должны выбирать и изменять свои пароли?
7. Как осуществляется управление паролями?
8. В чем заключается политика чистого стола экрана?
9. Каковы особенности сетевой аутентификации (по сравнению с аутентификацией при доступе к отдельному компьютеру)? Какие виды такой аутентификации рекомендуется использовать?
10. Какие средства защиты применяются в современных сетях - интранетах и экстранетах?
11. Какими защитными мерами осуществляется управление доступом к прикладным системам (приложениям)?
12. Как и на основе чего обеспечить ИВ при работе пользователей с переносными устройствами и в дистанционном режиме?
13. Какие процедуры при управлении защищенной передачей данных и операционной деятельности должны быть регламентированы?
14. Какие процедуры при управлении защищенной передачей данных и операционной деятельности должны быть регламентированы?
15. Какие мероприятия по управлению ИБ обеспечивают разделение сред разработки и промышленной эксплуатации систем?
16. Какие мероприятия по управлению ИБ обеспечивают разделение сред разработки и промышленной эксплуатации систем?
17. Что важно учитывать при планировании нагрузки и приемке систем?
18. На что необходимо обратить внимание при защите ПО и СОИ от вредоносных программ?
19. На основе чего осуществляется управление сетевыми ресурсами?
20. Как организуется защита носителей информации?
21. Как организуется защита носителей информации?
22. Что даст резервирование информации? Как правильно его организо-
23. Подробно рассмотрите процесс выработки требований к ИБ систем. Какие виды требований ИБ обычно должны быть определены?

24. Каковы области формулирования требований для эшелонированной защиты вычислительной среды организации?

25. Каковы области формулирования требований для эшелонированной защиты вычислительной среды организации?

26. Как обеспечивается ИБ системных файлов?

27. Кратко перечислите основные средства криптографической информа ции, используемые в сетевой среде.

28. Каковы основные цели и функции процессов управления конфигурациями, изменениями и обновлениями? Что между ними общего и в чем различия?

29. Опишите жизненный цикл процесса управления обновлениями ИБ. 30.Как осуществляется физическая зашита и зашита от воздействия

окружающей среды? В чем разница понятий логического и физического досту- па?

31. Как в организации создаются охраняемые зоны? Что такое периметр безопасности?

32. Как в организации создаются охраняемые зоны? Что такое периметр безопасности?

33. Дайте определения «ОИБ», «управления ИБ» и «СУИБ» организации. 34.Опишите деятельность ОИБ организации как процесс. Каковы его

входные и выходные данные, ресурсы и управляющие воздействия?

35. Как процесс ОИБ в организации связан с процессами основной деятельности организации?

36. Каковы основные этапы процесса управления ИБ ИТТ?

37. Что является хорошей практикой при выборе области действия СУИБ?

Какие стратегии выбор области действия СУИБ существуют?

38. Какие факторы необходимо учитывать при выборе области действия СУИБ?

39. Какие параметры процессов являются наиболее значимыми при выборе области действия проектируемой СУИБ?

40. Что входит в документальное обеспечение СУИБ? Каковы этапы её жизненного цикла?

### 7.2.6. Методика выставления оценки при проведении промежуточной аттестации

*Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.*

*1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.*

*2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов*

*3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.*

*4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)*

**7.2.7 Паспорт оценочных материалов**

| № п/п | Контролируемые разделы (темы) дисциплины | Код контролируемой компетенции | Наименование оценочного средства |
|---|---|---|---|
| 1 | Введение в теорию автоматического управления.Непрерывные системы управления. | ОПК-8, ОПК-4.1 | Тест, защита лабораторных работ |
| 2 | Дискретные системы управления | ОПК-8, ОПК-4.1 | Тест, защита лабораторных работ |
| 3 | Оптимальное управление | ОПК-8, ОПК-4.1 | Тест, защита лабораторных работ |
| 4 | Основы управления ИБ | ОПК-8, ОПК-4.1 | Тест, защита лабораторных работ |
| 5 | Управление рисками при обеспечении информа-ционной безопасности распределенных компью-терных систем | ОПК-8, ОПК-4.1 | Тест, защита лабораторных работ |
| 6 | Администрирование средств безопасности | ОПК-8, ОПК-4.1 | Тест, защита лабораторных работ |

**7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности**

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

## 8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

**8.1 Перечень учебной литературы, необходимой для освоения дисциплины**

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.

**8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:**

*Укажите перечень информационных технологий*

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/ (ЭБС IPRbooks)

## 9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

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

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

## 10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Теория управления информационной безопасностью компьютерных систем» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

| Вид учебных занятий | Деятельность студента |
|---|---|
| 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. |
| Лабораторная работа | Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания. |
| Самостоятельная работа | 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 промежуточной аттестации. |
| Подготовка к промежуточной аттестации | 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 экзаменом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала. |

## ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

| № п/п | Перечень вносимых изменений | Дата внесения изменений | Подпись заведующего кафедрой, ответственной за реализацию ОПОП |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |