МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____ /Гусев П.Ю./

28.02.2023 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 2023

Автор программы _____ К.А. Разинкин

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ К.А. Разинкин

Воронеж 2023

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
	навыками использования современных ИТ и технических средств для решения задач ИБ, а также методиками мониторинга эффективности защитных мер.

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: академические часы зач.ед.	 216 6	 108 3	 108 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. Непрерывные системы управления.	Роль и место дисциплины в программе подготовки специалиста. Дифференциальные уравнения физических систем. Статические и динамические характеристики систем. Линеаризация характеристик заданных графическии 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. Определение устойчивости по А.М.Ляпунову. Алгебраические критерии устойчивости систем автоматического управления. Частотные критериiустойчивости 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 системс применением интегрирующих устройств. Синтез систем с обратной связью по состоянию.	12	6	6	24

2	Дискретные системы управления	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 характеристика. Дискретная передаточная функция. Нули и полюса. Типовые переходные процессы. Моделив пространстве состояний. Физическая реализуемость. Устойчивость. Устойчивость поА.М. Ляпунову. Устойчивость линейных систем. Алгебраические критерии устойчивости.Критерий Михайлова. Критерий Найквиста.Одноконтурная дискретная система. Структурная схема.	12	6	6	24
3	Оптимальное управление	Постановка задачи управления. Функционал, его экстремум и вариация. Простейшая задачавариационного 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 приразличных режимах на концах оптимальной траектории. Задача с квадратичным функционалом. Принцип максимума для дискретных задач. Примеры решения задач. Динамическое программирование для линейной системы сквадратичным 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. МестоСУИБ 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 обеспечениюконтроля в отношении логического доступа. Контроль в отношении доступа пользователей. Обязанности пользователей. Контроль сетевого доступа. Контроль доступа к опера- ционной 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.	12	6	6	24
5	Управление рисками при обеспечении информационной безопасности рас- пределенных ком- пьютерных 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.	12	6	6	24

		Мониторинг, анализ и улучшение управлениярисками. Примеры типичных угроз. Уязви- мости и методы оценки уязвимостей. Подходык оценке риска ИБ.				
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 до- ступа и т.п.). Управление аутентификацией (распределение информации, необходимой для аутентификации - паролей, ключей и т.п.).Управление дополнением трафика (выработкаи поддержание правил, задающих характеристики дополняющих сообщений - частоту отправки, размер и т.п.). **Управление маршрутизацией** (выделение доверенных путей). Управление нотаризацией (распространение информации о нотариальных службах, адми- нистрирование этих служб).	12	6	6	24
		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».

Компе-тенция	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	описывает структуру системы управления ИБ и её связь с бизнес-процессами	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	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	обучающийся корректно подбирает математический аппарат для типовых задач управления безопасностью и применяет критерии оценки работоспособности динамических систем.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками использования современных критериев и стандартов для анализа безопасности распределенных компьютерных систем, проведения анализа рисков и администрирования безопасности распределенных компьютерных систем	владеет практическими приемами конфигурирования систем защиты и методами мониторинга безопасности в распределенной среде в соответствии с современными критериями и стандартами в области анализа рисков	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)	обучающийся способен системно изложить цели обеспечения триады ИБ (конфиденциальность, целостность, доступность) и классифицировать задачи управления защитой в ИКТ-среде в соответствии с нормативными стандартами и жизненным циклом систем.	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	обучающийся демонстрирует способность практически реализовать комплекс мер по защите сетевой инфраструктуры, успешно настраивая программно-аппаратные средства защиты и применяя методики разграничения доступа, шифрования и фильтрации трафика в соответствии с заданными политиками безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеет навыками использования современных ИТ и технических средств для решения задач ИБ, а также методиками мониторинга эффективности защитных мер.	обучающийся демонстрирует опыт эксплуатации актуальных программно-технических комплексов защиты и инструментов автоматизированного контроля, позволяющих проводить непрерывный мониторинг состояния системы, своевременно обнаруживать инциденты и оценивать реальную эффективность принятых мер безопасности на основе количественных и качественных показателей.	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	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	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	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 безопасности распределенных компьютерных систем, 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	Задачи не решены
ОПК-4.1	знать цели и задачи управления информационной безопасностью компьютерных систем (связь, информационны	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	е и коммуникационные технологии)					
	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
	владение навыками использования современных ИТ и технических средств для решения задач ИБ, а также методиками мониторинга эффективности защитных мер.	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	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 дистанционным; автоматизированным; автоматическим телемеханическим; централизованным.
2	Замкнутой системой по отклонению называется такая система, в которой: на вход автоматического регулятора поступает сумма задающего и возмущающего воздействий; на вход автоматического регулятора поступает сумма нескольких задающих воздействий с разными знаками;

	на вход автоматического регулятора поступает разность задающего воздействия и выходной величины; на вход автоматического регулятора поступает сумма задающего, возмущающего воздействий и выходной величины; на вход автоматического регулятора поступает задающее воздействие.
3	Разомкнутой системой первого рода называется такая система, в которой: на вход автоматического регулятора поступает сумма задающего и возмущающего воздействий; на вход автоматического регулятора поступает сумма нескольких задающих воздействий с разными знаками; на вход автоматического регулятора поступает разность задающего воздействия и выходной величины; на вход автоматического регулятора поступает сумма задающего, возмущающего воздействий и выходной величины; на вход автоматического регулятора поступает задающее воздействие.
4	Система автоматического регулирования, которая характеризуется произвольным законом изменения задающего воздействия во времени, называется: следящей; статической; астатической; программной; системой стабилизации.
5	Система автоматического регулирования, в которой задающее воздействие постоянно во времени, называется: следящей; статической; астатической; программной; системой стабилизации.
6	Система автоматического регулирования, в которой задающее воздействие изменяется по заранее заданному закону, называется: следящей; статической; астатической; программной; системой стабилизации.

7	Системой стабилизации называется: автоматическая система, в которой отсутствует обратная связь; автоматическая система, в которой задающее воздействие постоянно; автоматическая система, в которой задающее воздействие изменяется по заранее заданному закону; автоматическая система, на которую не воздействуют внешние возмущающие воздействия; автоматическая система, в которой задающее воздействие изменяется по случайному закону.
8	Нелинейной называется такая система автоматического регулирования: которая обладает способностью приспосабливаться к изменению внешних условий; все параметры которой изменяются во времени; которая описывается линейными дифференциальными уравнениями любого порядка; в которой все звенья описываются уравнениями вида y=kx; в состав которой входит хотя бы одно звено, описываемое нелинейными уравнениями
9	Импульсной называется такая система автоматического регулирования которая обладает способностью приспосабливаться к изменению внешних условий; все параметры которой изменяются во времени; которая описывается линейными дифференциальными уравнениями любого порядка; в состав которой входит хотя бы одно импульсное звено; в состав которой входит хотя бы одно звено, описываемое уравнениями вида y=kx.
10	Объектом регулирования называется устройство, совокупность устройств или часть устройства предназначенное для обеспечения заданных параметров качества процесса регулирования; устройство, совокупность устройств или часть устройства предназначенное для выполнения рабочей операции; устройство, совокупность устройств или часть устройства имеющее две входные величины;

	устройство, совокупность устройств или часть устройства выполняющее операцию сравнения входной и выходной координаты; устройство, совокупность устройств или часть устройства обеспечивающее требуемые параметры качества технологического процесса

7.2.3 Примерный перечень заданий для решения прикладных задач

ОПК-8 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	
1.	В распределенной банковской системе, состоящей из нескольких дата-центров, произошел сбой протокола синхронизации времени (NTP). Через некоторое время служба безопасности зафиксировала, что несколько транзакций были отклонены, а некоторые токены аутентификации стали недействительны. Какой фундаментальный принцип теории управления распределенными системами был нарушен, что привело к сбою в безопасности? 1.Принцип наблюдаемости (logs не собирались) 2.Нарушение глобальной синхронизации часов (отсутствие единого согласованного времени для формирования меток транзакций и времени жизни токенов) 3.Принцип обратной связи по возмущению
2.	Распределенная база данных системы управления спутниковой связью использует алгоритм консенсуса для подтверждения записей о состоянии каналов. Один из трех управляющих узлов был скомпрометирован и начал рассылать ложные данные. Какое свойство системы управления распределенной ИБ должно было сработать, чтобы сохранить целостность информации? 1.Византийская отказоустойчивость (Byzantine Fault Tolerance) системы, позволяющая достичь консенсуса даже при наличии ложных узлов 2.Резервное копирование на ленту 3.Повышение пропускной способности каналов
3.	Система обнаружения вторжений (IDS) распределена по филиалам в Москве и Владивостоке. Данные телеметрии стекаются в центральный офис в Москве. Из-за большой задержки канала (RTT ~ 180 мс)

	алгоритмы машинного обучения в центре обнаруживают атаку на Владивосток спустя 20 минут после ее начала. Какое явление теории управления распределенными системами требует применения другого подхода? 1.Наличие транспортного запаздывания, требующее переноса части интеллекта (Edge Computing / Fog Computing) на периферию 2.Квантование сигнала по уровню 3Нелинейность характеристик детектирования
4.	В компании используется централизованный контроллер домена (Active Directory) в головном офисе. При обрыве канала связи с филиалом, сотрудники филиала не могут войти в систему и получить доступ к своим же локальным ресурсам, так как кеш учетных записей исчерпан. Какое решение с точки зрения теории управления распределенными ресурсами необходимо внедрить? 1.Построить второй оптоволоконный кабель 2.Перевести всех сотрудников на постоянную удаленную работу 3.Внедрить распределенную модель управления удостоверениями (например, с использованием контроллеров домена в филиалах или технологий локальных кешей с длительным сроком действия)
5.	Перед внедрением новой системы шифрования трафика во всех филиалах компании (100 узлов по всему миру) необходимо понять, не вызовет ли криптографическая нагрузка коллапс сети и не превысит ли задержка кодирования критических значений для VoIP-телефонии. Какой метод научного исследования в области управления распределенными системами следует применить? 1.Натурный эксперимент на боевой сети (включить всё сразу и смотреть) 2.Имитационное моделирование (Simulation) распределенной сети с учетом топологии, задержек и нагрузок 3.Опрос сотрудников о качестве связи
6.	В распределенной сети "Интернета вещей" (датчики на трубопроводе) используется протокол на основе UDP. Часть пакетов теряется, и центральный диспетчерский пункт не знает актуальное давление в трубе, пытаясь управлять задвижками на устаревших данных. Какая фундаментальная проблема распределенных систем управления безопасностью здесь проявилась? 1.Проблема "византийских генералов"

	2.Проблема согласованности состояния (state consistency) при ненадежных каналах связи 3.Проблема выбора лидера кластера
7.	На распределенный веб-сервис началась DDoS-атака. Один из серверов в кластере перегружен и вот-вот упадет, в то время как другие загружены на 20%. Какое управляющее воздействие, основанное на теории автоматического управления, должна принять система балансировки? 1.Отключить атакуемый сервер от электричества 2.Перераспределить нагрузку (ребалансировка), перенаправляя часть запросов с перегруженного узла на свободные (динамическая маршрутизация) 3.Заблокировать все входящие запросы
8.	При разработке новой защищенной mesh-сети для МЧС (самовосстанавливающейся сети) ставится задача: найти путь передачи данных в обход узлов, которые перестали отвечать (подавлены или взломаны). Какой классический метод теории управления и исследования операций лежит в основе решения такой задачи? 1.Метод последовательных уступок 2.Алгоритмы поиска кратчайших путей на графе (например, алгоритм Дейкстры или Беллмана-Форда) с отбрасыванием "плохих" вершин 3.Метод Монте-Карло
9.	В распределенной системе шифрования дисков (например, для Kubernetes) необходимо организовать хранение мастер-ключа так, чтобы он был доступен всегда, но при этом злоумышленник не мог его украсть, скомпрометировав один сервер. Какой подход теории управления распределенными секретами (научная разработка) следует применить? 1.Хранить ключ на флешке у администратора 2.Использовать пороговую криптографию (Shamir's Secret Sharing), где секрет разделен на части, хранящиеся на разных узлах, и для восстановления требуется кворум (например, 3 из 5) 3.Отказаться от шифрования
10	Задание 10 (Метод анализа иерархий для выбора архитектуры) Научный сотрудник (ваша роль в рамках ОПК-8) стоит перед выбором архитектуры распределенной системы управления доступом: централизованная (проще, но единая точка отказа) или

	децентрализованная (сложнее, но надежнее). Критерии: стоимость, безопасность, скорость, масштабируемость. Применение какого научного метода позволит обоснованно выбрать оптимальный вариант? 1.Метод полного перебора 2.Метод анализа иерархий (МАИ) Томаса Саати (попарное сравнение критериев и альтернатив) 3.Голосование среди коллег
ОПК-4.1 - Способен организовывать защиту информации в компьютерных системах и сетях (связь, информационные и коммуникационные технологии)	
1.	Крупный холдинг имеет головной офис и 5 удаленных филиалов, соединенных через интернет. После атаки на филиал в Нижнем Новгороде вирус-шифровальщик смог пройти в головной офис и зашифровать базы 1С. Как необходимо организовать сеть, чтобы локализовать такие угрозы? 1.Увеличить скорость интернета в филиалах 2.Внедрить межсетевые экраны между филиалами и головным офисом, организовать VLAN'ы и строго сегментировать трафик по принципу "доверяй, но проверяй" 3.Отключить интернет в филиалах
2.	Компания использует общедоступные Wi-Fi сети в бизнес-центрах для подключения к корпоративным ресурсам. Перехваченный трафик одного из директоров позволил злоумышленникам получить доступ к коммерческой тайне. Как организовать защищенный удаленный доступ для сотрудников? 1.Запретить работу вне офиса 2.Выдать сотрудникам ноутбуки с предустановленным антивирусом 3.Организовать корпоративный VPN-сервер с шифрованием (IKEv2/IPsec или OpenVPN) и обязать всех сотрудников подключаться только через него
3.	На газопроводе используется распределенная система управления технологическим процессом (SCADA). Станции управления соединены по радиоканалу. Выявлено, что злоумышленник может подменить сигналы с датчиков давления. Какой комплекс мер необходимо организовать для защиты каналов связи? 1.Установить более мощные антенны

	2.Внедрить шифрование и имитозащиту (проверку подлинности) всех пакетов данных, передаваемых по радиоканалу 3.Перейти на проводную связь
4.	В распределенной сети базовых станций сотового оператора в одном из районов произошло отключение электричества на 6 часов. Аккумуляторы продержались 2 часа, станция отключилась, регион остался без связи. Как организовать энергоснабжение критических элементов распределенной сети? 1.Установить более мощные аккумуляторы 2.Организовать резервирование электропитания: дизель-генераторы на ключевых узлах и контракты на дозаправку, а также мониторинг остаточного заряда 3.Попросить МЧС подвозить бензин
5.	У компании 5000 торговых терминалов (касс) в магазинах по всей стране, работающих на устаревшей ОС Windows Embedded. Централизованно обновлять их сложно из-за низкой скорости каналов связи. На терминалах обнаружена критическая уязвимость. Как организовать процесс обновления безопасности в такой распределенной системе? 1.Обновлять только терминалы в головном офисе 2.Развернуть систему централизованного управления обновлениями (SCCM или аналог) с использованием механизмов peer-to-peer (Windows BranchCache) или локальных репозиториев в крупных хабах 3.Разослать обновления на флешках курьерской почтой
6.	Компания использует распределенную архитектуру микросервисов в облаке (Kubernetes). Неизвестно, как гарантировать, что в контейнерах с приложениями не запущен вредоносный код, измененный хакерами. Как организовать защиту на этапе развертывания? 1.Довериться облачному провайдеру 2.Внедрить в CI/CD пайплайн проверку цифровых подписей образов контейнеров и сканирование уязвимостей (Trivy, Clair) перед деплоем 3.Периодически останавливать все контейнеры и проверять вручную
7.	В распределенной сети госучреждения (областной центр + районы) происходит утечка персональных данных граждан. Определить, из какого именно филиала и через какого сотрудника уходят данные, невозможно. Какую систему необходимо организовать для выявления источника утечек?

	1.Запретить интернет во всех филиалах 2.Внедрить распределенную DLP-систему с агентами на всех рабочих станциях и центральной консолью в головном офисе, настроить политики и маркировку документов 3.Установить видеокамеры у всех принтеров
8.	Система дистанционного банковского обслуживания (ДБО) для корпоративных клиентов использует только логин и пароль. Участились случаи взлома и хищения денег. Как организовать защиту доступа к распределенным финансовым сервисам? 1.Усложнить требования к паролям (заглавные, цифры, спецсимволы) 2.Обязательно внедрить двухфакторную аутентификацию (2FA) с использованием одноразовых кодов (SMS, Push-уведомления, аппаратные токены) для всех критических операций 3.Перевести всех клиентов на бумажную отчетность
9.	В филиале во Владивостоке произошел серьезный инцидент ИБ (атака на серверы). Специалисты по реагированию находятся только в Москве. Пока они летели (9 часов), филиал работал и улики были уничтожены. Как организовать процесс реагирования в географически распределенной компании? 1.Смириться с потерей времени 2.Создать распределенную команду реагирования (CSIRT) с обученными сотрудниками в каждом крупном филиале и разработать четкие playbooks для первичных действий до приезда центральной команды 3Закрыть филиал во Владивостоке
10	У компании парк оборудования разных вендоров (Cisco, Huawei, Juniper) в 20 городах. При инциденте безопасности приходится заходить на каждое устройство вручную, чтобы найти логи, что занимает дни. Как организовать централизованный мониторинг событий ИБ в распределенной сети? 1.Установить стандартные пароли на всё оборудование для быстрого доступа 2.Свести всю информацию в Excel

	3Внедрить распределенную SIEM-систему (или систему сбора логов на базе Elastic Stack/Splunk) с агентами или приёмом syslog со всех устройств в единый центр

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень вопросов для подготовки к экзамену

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 информации, 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 доступа?

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, 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 информационной безопасности распределенных компьютерных 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:

Системы управления информационной безопасностью и соответствия
IBM QRadar SIEM https://www.ibm.com/products/qradar-siem
Splunk Enterprise Security
https://www.splunk.com/en_us/software/enterprise-security.html
MaxPatrol SIEM (Positive Technologies)
https://www.ptsecurity.com/ru-ru/products/maxpatrol/

Системы управления рисками (GRC)
RSA Archer GRC https://www.archerirm.com/
ServiceNow Governance, Risk, and Compliance (GRC)
https://www.servicenow.com/products/governance-risk-and-compliance.html

Средства защиты распределенных систем и сетей
UserGate https://www.usergate.com/ru/products

Системы защиты от утечек (DLP)
Symantec Data Loss Prevention
https://www.broadcom.com/products/cybersecurity/data-loss-prevention

Стандарты и методологии (документы)
ISO/IEC 27001
https://www.iso.org/isoiec-27001-information-security.html
NIST Cybersecurity Framework
https://www.nist.gov/cyberframework

ГОСТ Р ИСО/МЭК 27001-2021
https://protect.gost.ru/default.aspx

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: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - 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