Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И УПРАВЛЯЮЩИХ СИСТЕМ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.О.13.06 «СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор Стрельцова Г.А. Рабочая программа дисциплины: Сети и системы передачи информации. – Королев МО: «Технологический университет», 2023.

Рецензент: **Артюшенко В.М.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Артюшенко В.М. д.т.н., профессор			
Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания кафедры	№12 от 05.04.2023			

Рабочая программа согласована:

Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания УМС	№5 от 11.04.2023			

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП

Целями изучения дисциплины является:

1. Изучение основных принципов построения систем передачи информации;
2. Понимание структуры систем и сетей связи;
3. Ознакомление с принципами работы технических устройств и средств, входящие в их состав.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;

Основными **задачами** дисциплины являются:

1. Получение знаний о технологиях передачи информации;
2. Приобретение навыков защиты беспроводных сетей;
3. Умение работать с программными продуктами и оборудованием; предназначенными для передачи информации.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- описание сути проблемной ситуации
- знает принципы построения систем и сетей электросвязи;
- знает современные виды информационного взаимодействия и обслуживания телекоммуникационных сетей и систем;
- знает основные понятия и задачи криптографии, математические модели криптографических систем
- знает основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы
- знает национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения
- знает классификацию и количественные характеристики технических каналов утечки информации;
- знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;
- знает организацию защиты информации от утечки по техническим каналам на объектах информатизации;

Необходимые умения:

- выявление составляющих проблемной ситуации и связей между ними
- умеет проводить анализ показателей эффективности сетей и систем телекоммуникаций и качества предоставляемых услуг;
- умеет применять математические модели для оценки стойкости СКЗИ
- умеет использовать СКЗИ в автоматизированных системах

Трудовые действия:

- выбор способа обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации
- сбор и систематизация информации по проблеме
- оценка адекватности и достоверности информации о проблемной ситуации
- выбор методов критического анализа, адекватных проблемной ситуации
- разработка и обоснование плана действий по решению проблемной ситуации
- владеет методами и средствами технической защиты информации.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Сети и системы передачи информации» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория вероятностей и математическая статистика», «Теория информации», «Языки программирования», «Технологии и методы программирования», «Аппаратные средства вычислительной техники» и компетенциях: ОПК-2,3,7,9,11.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Информационная безопасность автоматизированных систем», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 4 зачётных единиц, 144 часа.

Таблица 1

Виды занятий	Всего часов	Семестр 6	Семестр 7	Семестр 8	Семестр …
Общая трудоемкость	144	144		144	
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	64	64			
Лекции (Л)	32	32			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	16	16			
Другие виды контактной работы					
Практическая подготовка	нет	нет			
Самостоятельная работа	70	72			
Курсовые, расчетно-графические работы	12	12-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели) – 2часа	Тест Т-1;Т-2.	Тест Т-1;Т-2.			
Вид итогового контроля	Экзамен	Экзамен			
ОЧНО-ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	32			32	
Лекции (Л)	16			16	
Практические занятия (ПЗ)	8			8	
Лабораторные работы (ЛР)	8			8	
Другие виды контактной работы	12			12	
Практическая подготовка	нет			нет	
Самостоятельная работа	110			110	
Контроль самостоятельной работы	-			-	
Курсовые, расчетно-графические работы	-			-	
Контрольная работа, домашнее задание	+			+	
Вид итогового контроля	Экзамен			Экзамен	

Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очная/очно-заочная	Лабораторные работы, час. Очная/очно-заочная	Практические занятия, час. Очная/очно-заочная	Занятия в интерактивной форме, час.	Код компетенций
Тема 1. Общие сведения о системах передачи информации	2/1	1/1	1/1	2/-	УК-1
Тема 2. Введение в теорию сигналов и систем	4/1	1/1	1/1	2/1	УК-1
Тема 3. Кодирование источников сообщений и каналов связи	4/1	2/1	2/1	2/1	УК-1
Тема 4. Методы модуляции.	4/1	2/1	2/1	2/1	УК-1
Тема 5. Принципы построения сетей связи	4/2	2/1	2/1	2/1	ОПК-9
Тема 6. Основные характеристики сетей связи	4/2	2/1	2/1	2/1	ОПК-9
Тема 7. Многоканальные системы связи	4/2	2/1	2/1	2/1	ОПК-9
Тема 8. Принципы построения систем радиосвязи	4/2	2/0.5	2/0.5	2/0.5	ОПК-9
Тема 9. Особенности построения информационно-	2/4	2/0.5	2/0.5	2/0.5	ОПК-9

вычислительных систем					
Итого:	32/16	16/8	16/8	18/8	

4.2. Содержание тем дисциплины

Тема 1. Общие сведения о системах передачи информации

Основные понятия и определения. Структура передачи сообщений. Количественные характеристики источников информации. Особенности образования и характеристики речевых сигналов.

Тема 2. Введение в теорию сигналов и систем

Общие сведения и понятия. Классификация сигналов. Преобразование типа сигналов. Энергетические спектры сигналов. Методы аналого-цифрового преобразования сигналов.

Тема 3. Кодирование источников сообщений и каналов связи

Основные понятия и классификация методов кодирования. Основы экономного кодирования (коды без памяти, коды Хаффмена, коды с памятью, арифметическое кодирование, словарные методы кодирования, кодирование длин повторений). Основы помехоустойчивого кодирования (линейные блочные коды, циклические коды, сверточные коды, применение корректирующего кодирования в системах).

Тема 4. Методы модуляции. Основные понятия

Виды модуляции. Сигналы при непрерывной модуляции. Сигналы при импульсной модуляции. Сигналы при дискретной модуляции. Методы модуляции с расширением спектра.

Тема 5. Принципы построения сетей связи

Функциональный состав сети связи (терминалы связи, системы передачи, системы коммутации). Классификация сетей связи. Современные виды информационного обслуживания (традиционные службы, телематические службы, сети связи с интеграцией служб).

Тема 6. Основные характеристики сетей связи

Морфологические характеристики сети связи (архитектура, структура, топология). Характеристики целевого предназначения сети связи (пропускная способность, живучесть). Технико-эксплуатационные характеристики сетей связи (функционирующая в сети связи нагрузка, надёжность функционирования сети связи).

Тема 7. Многоканальные системы связи

Принципы построения современных многоканальных систем передачи. Частотное и временное разделение каналов). Проводные и волоконно-оптические линейные тракты.

Тема 8. Принципы построения систем радиосвязи

Особенности распространения радиоволн. Структура средств радиосвязи. Системы связи: радиорелейной, тропосферной, спутниковой.

Тема 9. Особенности построения информационно-вычислительных систем (ИВС)

Эталонная модель взаимодействия открытых систем. Назначение и классификация ИВС. Технические устройства ИВС (назначение компьютеров в сети, коммуникационное оборудование, сетевые программные средства, основные стеки сетевых протоколов, технологии локальных сетей, маршрутизация в ИВС).

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

1. «Методические указания для обучающихся по освоению дисциплины» приведены в приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю) приведена в Приложении 1 к настоящей программе.

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

Основная литература:

1.Антонов, Д. А. Применение коммутаторов в современных сетях передачи информации : учебно-методическое пособие / Д. А. Антонов, А. Е. Ермакова, С. Е. Иконников. — Москва : РУТ (МИИТ), 2021. — 94 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/269750 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

2.Лебедько, Е. Г. Теоретические основы передачи информации : монография / Е. Г. Лебедько. — Санкт-Петербург : Лань, 2022. — 352 с. — ISBN 978-5-8114-1139-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/210620 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

3.Зверева, Е. Н. Сборник примеров и задач по основам теории информации и кодирования сообщений : учебно-методическое пособие / Е. Н. Зверева, Е. Г. Лебедько. — Санкт-Петербург : НИУ ИТМО, 2014. — 76 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/71068 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

4.Устиновский, Е. П. Проектирование цепных передач с применением ЭВМ : учебное пособие / Е. П. Устиновский, Е. В. Вайчулис, А. В. Ковнацкий. — Челябинск : ЮУрГУ, 2017. — 132 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167542 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

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

Интернет-ресурсы:

1. http://www. eup.ru–научно-образовательный портал.
2. http://www. informika.ru– образовательный портал.
3. Материалы сайта studentsworks/
4. Материалы сайта cooldoclad.narod/

9. Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения: MSOffice, PowerPoint.

Информационные справочные системы:

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды Университета
2. Рабочая программа и методическое обеспечение по дисциплине «Сети и системы передачи информации».
3. Программные продукты: САПР «Эксперт СКС»
4. Электронные ресурсы образовательной среды Университета.
5. Рабочая программа и методическое обеспечение по дисциплине: «Сети и системы передачи информации».

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

– аудитория, оснащенная презентационной техникой (проектор, экран);

– комплект электронных презентаций / слайдов на темы:

Практические занятия:

– аудитория, снабжённая достаточным количеством посадочных мест, исходя из списочной численности группы;

– рабочее место преподавателя»

– рабочие места студентов, оснащенные компьютерами с доступом в глобальную сеть Интернет;

– медиа-проектор, компьютер, аудио-оборудование – в специально оговорённых случаях.

Приложение 1

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

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И УПРАВЛЯЮЩИХ СИСТЕМ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

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

№ п/п	Индекс компе-тенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Тема 1,2,3,4.	- выбор способа обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации - сбор и систематизация информации по проблеме - оценка адекватности и достоверности информации о проблемной ситуации	- выявление составляющих проблемной ситуации и связей между ними	- описание сути проблемной ситуации
2.	ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	Тема 1,2,3,4,5,	- владеет методами и средствами технической защиты информации	- умеет проводить анализ показателей эффективности сетей и систем телекоммуникаций и качества предоставляемых услуг; - умеет применять математические модели для оценки	- знает принципы построения систем и сетей электросвязи; - знает современные виды информационного взаимодействия и обслуживания телекоммуникационных сетей и систем; - знает основные понятия и задачи

№ п/п	Индекс компе-тенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает		
				Трудовые действия	Необходимые умения	Необходимые знания
					стойкости СКЗИ - умеет использовать СКЗИ в автоматизированных системах - умеет анализировать и оценивать угрозы информационной безопасности объекта информатизации;	криптографии, математические модели криптографических систем - знает основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы знает национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения

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

Код компетенции	*Инструмент, оценивающий сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
УК-1; ОПК-9	*Доклад*	*А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов* *Б) частично сформирована:* • *компетенция освоена на <u>продвинутом</u> уровне – 4 балла;* • *компетенция освоена на <u>базовом</u> уровне – 3 балла;* *В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов*	*Например:* ***Проводится в письменной и/или устной форме.*** *Критерии оценки:* *1. Соответствие содержания доклада заявленной тематике (1 балл).* *2. Качество источников и их количество при подготовке работы (1 балл).* *3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).* *4. Качество самой представленной работы (1 балл).* *5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).* ***Максимальная сумма баллов - 5 баллов.***
УК-1; ОПК-9	***Выполнение контрольной работы***	*А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов* *Б) частично сформирована:* • *компетенция освоена на <u>продвинутом</u> уровне – 4 балла;* • *компетенция освоена на <u>базовом</u> уровне – 3 балла;* *В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов*	*При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида*
УК-1; ОПК-9	*Лабораторная*	*А) полностью*	*Например:*

Код компетенции	*Инструмент, оценивающий сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
	работа	*сформирована (компетенция освоена на высоком уровне) – 5 баллов* *Б) частично сформирована:* • *компетенция освоена на продвинутом уровне – 4 балла;* • *компетенция освоена на базовом уровне – 3 балла;* *В) не сформирована (компетенция не сформирована) – 2 и менее баллов*	*1. Оформление в соответствии с требованиями (1 балл).* *2. Выбор методов измерений и вычислений (1 балл).* *3. Умение применять выбранные методы (1 балл).* *4. Анализ и выводы, отражающие суть изучаемого явления с указанием конкретных результатов (2 балла).* *Максимальная оценка – 5 баллов.*

3. Типовые контрольные, практические задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Информационная безопасность сетевого периметра организации на основе применения технологии «тонкого клиента».
2. Информационная безопасность системы «клиент – банк» на основе технологии «толстого клиента».
3. Базовая модель угроз для информационных систем, обрабатывающих персональные данные.
4. Базовая модель угроз для государственных информационных систем.
5. Возможные модели нарушителей сетевого периметра организации.
6. Информационная безопасность модели Интернет - банкинга.
7. Информационная безопасность расчетов банковскими картами в Интернете.
8. Управление информационной безопасностью в организации.
9. Оценка и обработка рисков информационной безопасности.
10. Управление рисками информационной безопасности.
11. Документальное и инструментальное обеспечение управления рисками информационной безопасности.
12. Классификация технических каналов утечки информации для информационных систем.

13. Физическая природа побочных электромагнитных излучений в технических средствах обработки информации.
14. Наводки электромагнитных излучений при обработке информации в информационных системах.
15. Технические каналы утечки информации при передаче ее по каналам связи.
16. Средства выявления каналов утечки информации.
17. Технический контроль эффективности мер защиты информации.
18. Скрытие и защита информации от утечки по техническим каналам.
19. Защита информационных систем от несанкционированного доступа.
20. Классификация АС, СВТ и МЭ по требованиям защиты информации от несанкционированного доступа.
21. Классификация ПО по уровню контроля отсутствия не декларированных возможностей.
22. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
23. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
24. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
25. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
26. Функция хеширования и ассиметричные алгоритмы.
27. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
28. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
29. Информационная безопасность при составление и направление ЭД участником – отправителем.
30. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
31. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Сети и системы передачи информации» являются две текущие аттестации в виде тестов в течение каждого семестра и итоговые аттестации в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	УК-1; ОПК-9	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	УК-1; ОПК-9	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***
Проводится в сроки, установленные графиком образо	Экзамен	УК-1; ОПК-9	3 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время,	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: 1. знание основных понятий предмета;

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
вательного процесса				отведенное на процедуру – 30 минут.		2. умение использовать и применять полученные знания на практике; 3. работа на практических занятиях; 4. знание основных научных теорий, изучаемых предметов; 5. ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
						«У**довлетворительно**»: 1. демонстрирует частичные знания по темам дисциплин; 2. незнание неумение использовать и применять полученные знания на практике; 3. не работал на практических занятиях; «**Неудовлетворительно**»: 4. демонстрирует частичные знания по темам дисциплин; 5. незнание основных понятий предмета; 6. неумение использовать и применять полученные знания на практике; 7. не работал на практических занятиях; 8. не отвечает на вопросы.

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

1. Функции КСЗИ:
   создание механизмов защиты, сводящие до минимума возможность воздействия дестабилизирующих факторов на защищаемую информацию; непрерывное и оптимальное управление механизмами комплексной защиты +
   обеспечение конфиденциальности, целостности, доступности информации
   обеспечение криптографической, программной и аппаратной защиты информации
   обеспечение защиты людей, материальных носителей, автоматизированных систем

2. Требование безопасности повторного использования объектов противоречит:
   инкапсуляции +
   наследованию
   полиморфизму

3. Уровни модели OSI, по возрастанию:
   физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной +
   сетевой, канальный, транспортный, сеансовый, прикладной, представления, физический
   прикладной, представления, физический, канальный, сетевой, транспортный, сеансовый
   физический, сетевой, канальный, транспортный, сеансовый, представления, прикладной

4. Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:
   запрет на чтение каких-либо файлов, кроме конфигурационных
   запрет на изменение каких-либо файлов, кроме конфигурационных +
   запрет на установление сетевых соединений

5. Уровни модели TCP/IP, по возрастанию:
   канальный, сетевой, транспортный, прикладной +
   транспортный, канальный, сетевой, прикладной
   канальный, транспортный, сетевой, прикладной
   прикладной, сетевой, транспортный, канальный

6. К какому уровню модели TCP\IP относятся следующие протоколы HTTP, RTP, FTP, DNS:
   прикладной +
   транспортный

сетевой
канальный

7. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
меры обеспечения целостности
административные меры +
меры административного воздействия

8. Что входит в функции систем мониторинга:
выявление состояния систем
установка отношений между объектами
установка соответствия правил и обязанностей
все варианты верны +

9. Какие существуют подходы по построению защищенных операционных систем применяемых в АС:
фрагментарный и комплексный +
фрагментарный и операционный.
комплексный и позиционный.
системный и позиционный.

10. Дублирование сообщений является угрозой:
доступности
конфиденциальности
целостности +

11. Какие существуют методы оценки качества КСИБ:
метод оценки уязвимости Хоффмана +
экспертная оценка +
сигнатурный метод
качественный метод.

12. Самыми опасными источниками внутренних угроз являются:
некомпетентные руководители +
обиженные сотрудники
любопытные администраторы

13. Для внедрения бомб чаще всего используются ошибки типа:
отсутствие проверок кодов возврата
переполнение буфера +
нарушение целостности транзакций

14. В число целей политики безопасности верхнего уровня входят:
решение сформировать или пересмотреть комплексную программу безопасности +
обеспечение базы для соблюдения законов и правил +
обеспечение конфиденциальности почтовых сообщений

15. В число целей программы безопасности верхнего уровня входят:
управление рисками +
определение ответственных за информационные сервисы
определение мер наказания за нарушения политики безопасности

16. Что означает обеспечение целостности баз данных.

это соответствие информации базы данных её внутренней логике, структуре и заданным правилам. +
это полное значение информации базы данных в котором действуют установленные правила
это информация, работающая по установленной структуре базы данных.
это логическая операция обеспечивающая полноту информации и соблюдающая условия того, что информация не будет изменена.

17. В рамках программы безопасности нижнего уровня осуществляются:
стратегическое планирование
повседневное администрирование +
отслеживание слабых мест защиты +

18. Политика безопасности строится на основе:
общих представлений об ИС организации
изучения политик родственных организаций
анализа рисков +

19. В число целей политики безопасности верхнего уровня входят:
формулировка административных решений по важнейшим аспектам реализации программы безопасности +
выбор методов аутентификации пользователей
обеспечение базы для соблюдения законов и правил +

20. Основные механизмы защиты применяемые в ОС:
идентификации / аутентификации
разграничения доступа
аудита
все перечисленные варианты верны +

4.3. Типовые вопросы, выносимые на экзамен

1. Предмет, цель и задачи обеспечения информационной безопасности в организации.

2. Дайте определение конфигурации информационных ресурсов компьютерных систем, в чем заключается их администрирование.

3. Дайте определение и приведите классификацию угроз безопасности информации для информационных систем.

4. Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации.
5. Идентификация и аутентификация субъектов доступа и объектов доступа.
6. Управление доступом субъектов доступа к объектам доступа.
7. Ограничение программной среды в защищенных АС.
8. Защита машинных носителей информации в АС.
9. Регистрация событий безопасности в информационной системе.
10. Антивирусная защита в информационной системе.
11. Обнаружение (предотвращение) вторжений в информационную систему.
12. Контроль защищенности информации в информационной системе.
13. Обеспечение целостности информационной системы и информации
14. Обеспечение доступности информации в информационной системе.
15. Защита информационной системы, ее средств и систем связи и передачи данных.
16. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.
17. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.
18. Базовая модель угроз ИСПДн.
19. Уязвимости АС, возможные атаки на них.
20. Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.
21. Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.
22. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.
23. Классификация методов криптографического закрытия информации.
24. Аппаратные и программные средства реализации шифров.

25. Особенности использования вычислительной техники в криптографии; вопросы организации сетей связи с аппаратурой шифрования; ключевые системы.
26. Организация защиты в распределенных сетях с использованием виртуальных частных сетей.
27. Электронные цифровые подписи (электронные подписи).
28. Криптографические хеш-функции.
29. Криптографические протоколы.
30. Основные подходы к реализации PKI.
31. Симметричные криптосистемы.
32. Симметричные методы шифрования.
33. Алгоритмы блочного шифрования.
34. Режимы применения блочных шифров.
35. Потоковые шифры.
36. Комбинированные методы шифрования.
37. Асимметричные системы шифрования.
38. Применение асимметричных алгоритмов.
39. Средства криптографической защиты, разработанные компаниями: Инфотекс, Крипто-Про, ОКБ Сапр, Аладдин и Adobe, MS Windows, Cisco.
40. Хранилище сертификатов ОС MS Windows.

Типовые вопросы, выносимые на экзамен (часть 2)

1. Перечислите защитные механизмы, реализуемые программно-аппаратными комплексами (средствами) защиты информации в компьютерных системах (ПЭВМ). Дайте определение понятию - «субъект доступа», какие процедуры реализуются при его обращении к компьютерной системе.
2. Перечислите методы противодействия дизассемблированию программ для ЭВМ, охарактеризуйте их.
3. В чем заключается процедура простой аутентификации, какими способами она производится, поясните схематично ее реализацию с использованием пароля.
4. Перечислите основные модели разграничения доступа, действующие в операционных системах, и поясните, в чем они заключаются. Дайте определение понятиям «матрица доступа» и «домен безопасности».

5. Поясните использование односторонней хэш-функции для проверки пароля при аутентификации пользователя ресурсов компьютерной системы.

6. Чем достигается защита средств управления, коммутации и внутреннего монтажа компьютерных систем (ПЭВМ), из чего состоит и как действует единая система контроля вскрытия устройств (СКВУ).

7. Для чего создается система разграничения доступа (СРД) компьютерной системы, какие функциональные блоки она включает. Поясните работу функциональной схемы диспетчера доступа.

8. В чем заключается биометрическая аутентификация пользователей, какие у нее достоинства и недостатки.

9. Дайте определение основным понятиям процесса разграничения доступа к объектам операционной системы (ОС): «объект доступа»; «метод доступа»; «субъект доступа»; «право доступа». Каким требованиям должны удовлетворять правила разграничения доступа.

10. Приведите примеры сущностей субъекта доступа для подтверждения своей подлинности при осуществлении аутентификации в компьютерной системе (ПЭВМ).

11. Какими способами блокируется угроза несанкционированного копирования информации ПЭВМ, в чем они заключаются, раскройте их содержание.

12. В зависимости от предъявления субъектом доступа каких сущностей можно разделить процессы аутентификации в компьютерных системах (ПЭВМ)?

13. Основные подходы к защите данных от НСД: какие действия выполняются при организации доступа к оборудованию и ПО компьютерных систем (ПЭВМ); оценка эффективности наращивания средств контроля доступа по кривой роста относительного уровня обеспечения безопасности компьютерных систем (ПЭВМ).

14. Перечислите атрибутивные идентификаторы, используемые для идентификации субъекта доступа в КС, и коротко дайте им определение.

15. Какие основные функции выполняет подсистема защиты операционных систем (ОС), дайте коротко им определение. В чем заключается процедура аудита применительно к ОС, чем она обусловлена, каким требованиям она должна удовлетворять.

16. Какую последовательность действий включает общий алгоритм механизма защиты от несанкционированного использования программ в «чужой» среде.
17. Раскройте методы аутентификации, использующие пароли и PIN-коды.
18. Перечислите и раскройте способы строгой аутентификации.
19. Какие существуют криптосистемы шифрования, раскройте их смысл функционирования.
20. Раскройте основные процедуры формирования электронной цифровой подписи и функции хэширования.
21. Как осуществляется управление криптоключами, требования к распределению ключей, методы распределения ключей.
22. Раскройте классификацию и жизненный цикл компьютерных вирусов.
23. Перечислите методы ограничения доступа к компонентам ЭВМ, какие применяют средства для ограничения доступа к компонентам ЭВМ.
24. В чем заключается задача идентификации пользователя, дайте определение понятию протокола идентификации.
25. В чем заключается локальная и удаленная идентификация, что такое идентифицирующая информация.
26. Какие существуют способы хранения идентифицирующей информации, их связь с ключевыми системами.

**Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.*

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И УПРАВЛЯЮЩИХ СИСТЕМ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

1. Общие положения

Целями изучения дисциплины является:

– формирование базовых знаний и практических навыков обеспечения безопасности информационных систем;

– развитие творческого и исследовательского подхода к изучению технических дисциплин студенчества;

– подготовка студентов к видам профессиональной деятельности: проектной, производственно-технологической, организационно-управленческой, аналитической и научно-исследовательской;

– приобретение студентами знаний и представлений об основных принципах и закономерностях функционирования современной вычислительной техники;

– приобретение студентами теоретических сведений и практических навыков, позволяющих формировать устройства вычислительной техники с заданными техническими характеристиками.

Задачами дисциплины являются:

1. Формирование целостного компендиума знаний правовых и методических документов в области обеспечения безопасности информационных систем (ИС);
2. Изучение базовых моделей угроз информационной безопасности и возможных моделей нарушителей для обеспечения проектирования ИС;
3. Изучение национальных стандартов и методических положений по оценке информационной защищённости при анализе и проектировании защищённых ИС;
4. Подготовка студентов к деятельности, связанной с созданием, эксплуатацией и обслуживанием (сопровождением) защищённых ИС;
5. Привитие навыков работы с проектной и технической документацией по проектированию защищённых ИС и оценке их эффективности.
6. Формирование знаний по проведению аудита информационной безопасности в организации;
7. Изучение и привитие навыков применения национальных стандартов, нормативных и методических документов в области управления информационной безопасностью;
8. Формирование представлений о принципах обеспечения информационной безопасности при использовании вычислительной техники;
9. Изучение принципов построения и работы основных цифровых узлов;
10. Приобретение опыта выбора элементной базы и типовых

цифровых узлов вычислительной техники.

2. Указания по проведению практических занятий

Практическое занятие 1.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Предмет и задачи программно-аппаратной защиты информации.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Компьютерная система (КС). Структура и компоненты КС. Классы и типы КС. Сети ЭВМ.
2. Основные понятия программно-аппаратной защиты информации: электронный документ (ЭД) и их типы; виды информации в КС; информационные потоки в КС; понятие исполняемого модуля.
3. Уязвимость компьютерных систем: понятие доступа, субъект и объект доступа; понятие несанкционированного доступа (НСД); классы и виды НСД; несанкционированное копирование программ как особый вид НСД; понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).

Продолжительность занятия — 2/2 часа

Практическое занятие 2.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Идентификация пользователей КС - субъектов доступа к данным.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Понятие идентификации пользователя.
2. Задача идентификации пользователя.
3. Понятие протокола идентификации.
4. Локальная и удаленная идентификация.
5. Идентифицирующая информация. Понятие идентифицирующей информации.
6. Способы хранения идентифицирующей информации, связь с ключевыми системами.

Продолжительность занятия — 2/2 часа

Практическое занятие 3.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Средства и методы ограничения доступа к файлам.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Основные подходы к защите данных от НСД: шифрование; контроль доступа; разграничения доступа; файл как объект доступа; оценка надежности систем ограничения доступа - сведение к задаче оценки стойкости.

2. Организация доступа к файлам: иерархический доступ к файлам; понятие атрибутов доступа; организация доступа к файлам в различных ОС; защита сетевого файлового ресурса на примерах организации доступа в ОС UNIX, Novell NetWare и т. д.

3. Фиксация доступа к файлам: способы фиксации фактов доступа; журналы доступа; критерии информативности журналов доступа; выявление следов несанкционированного доступа к файлам; метод инициированного НСД.

4. Доступ к данным со стороны процесса: понятие доступа к данным со стороны процесса; отличия от доступа со стороны пользователя; понятие и примеры скрытого доступа; надежность систем ограничения доступа.

5. Особенности защиты данных от изменения: зашита массивов информации от изменения (имитозащита); криптографическая постановка защиты от изменения данных; подходы к решению задачи защиты данных от изменения; подход на основе формирования имитоприставки (МАС), способы построения МАС; подход на основе формирования хэш-функции, требования к построению и способы реализации; формирование электронной цифровой подписи (ЭЦП); особенности защиты ЭД и исполняемых файлов; проблема самоконтроля исполняемых модулей.

Продолжительность занятия — 2/2 часа

Практическое занятие 4.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Программно-аппаратные средства шифрования

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Построение программно-аппаратных комплексов шифрования: аппаратные и программно-аппаратные средства криптозащиты данных; построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования.

2. Защита алгоритма шифрования, принцип чувствительной области и принцип главного ключа.

3. Необходимые и достаточные функции аппаратного средства криптозащиты, проектирование модулей криптопреобразований на основе сигнальных процессоров.

4. Плата Криптон-3 (Криптон-4): архитектура платы; организация интерфейса с приложениями. 5. Другие программно-аппаратные СКЗД.

Продолжительность занятия — 2/2 часа

Практическое занятие 5.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Защита программ от несанкционированного копирования

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Несанкционированное копирование программ: несанкционированное копирование программ как тип НСД; юридические аспекты несанкционированного копирования программ; общее понятие защиты от копирования. Разновидности задач защиты от копирования.
2. Подходы к задаче защиты от копирования: привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО; привязка программ к гибким магнитным дискам (ГМД); структура данных на ГМД; управление контроллером ГМД; способы создания некопируемых меток; точное измерение характеристик форматирования дорожки; технология «слабых битов»; физические метки и технология работы с ними; привязка программ к жестким магнитным дискам (ЖМД); особенности привязки к ЖМД; виды меток на ЖМД; привязка к прочим компонентам штатного оборудования ПЭВМ; привязка к внешним (добавляемым) элементам ПЭВМ; привязка к портовым ключам; использование дополнительных плат расширения; методы «водяных знаков» и методы «отпечатков пальцев».

Продолжительность занятия — 2/2 часа

Практическое занятие 6.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Защита программ от излучения

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Изучение и обратное проектирование ПО: понятие изучения и обратного проектирования ПО; цели и задачи изучения работы ПО; способы изучения ПО: статическое и динамическое изучение; роль программной и аппаратной среды; временная надежность (невозможность обеспечения гарантированной надежности).
2. Задачи защиты от изучения и способы их решения: защита от отладки; динамическое преобразование кода; итеративный программный замок А. Долгина; принцип ловушек и избыточного кода; защита от дизассемблирования; принцип внешней загрузки файлов; динамическая модификация программы; защита от трассировки по прерываниям.
3. Аспекты проблемы защиты от исследования: способы ассоциирования защиты и программного обеспечения; оценка надежности защиты от отладки.
4. Вирусы: защита от разрушающих программных воздействий; вирусы как особый класс разрушающих программных воздействий; необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды.

Продолжительность занятия — 2/2 часа.

Практическое занятие 7.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам

Вид практического занятия: смешанная форма практического занятия.

Тема и содержание практического занятия: Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.

Требования, предъявляемые к формированию политики безопасности организации. Структура и содержание политики безопасности организации применительно к компьютерным системам.

Цель работы: получить практические знания и навыки об управлении информационной безопасностью и формированию политики информационной безопасности в организации.

Учебные вопросы:

1. Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.
2. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.
3. Требования, предъявляемые к формированию политики безопасности организации.
4. Структура и содержание политики безопасности организации применительно к компьютерным системам.
5. Цель работы: получить практические знания и навыки об управлении информационной безопасностью и формированию политики информационной безопасности в организации.

Продолжительность занятия — 2/1 часа.

Практическое занятие 8.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Методология обследования и проектирования защищенных информационных (автоматизированных) систем

Вид практического занятия: смешанная форма практического занятия.

Тема и содержание практического занятия: Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС. Принципы проектирования. Структурный принцип и принцип модульного проектирования. Три основных конструкции для проектирования. Преимущества использования модульного принципа.

Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта. Спецификация требований программного обеспечения.

Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной спецификации. Основные подходы к определению спецификаций требований.

Теория безопасных систем (TCB). Понятие «доверенная вычислительная среда» (trusted computing base-TCB). Дискретная природа характеристики «безопасный». Характеристика «доверенный». Доверенная вычислительная среда. Набор компонентов, составляющий доверенную вычислительную среду. Этапы разработки защищённой АС. Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2014). Цель создания АСЗИ.

Цель работы: получить практические знания и навыки об этапах и содержании работ по проектированию защищенных информационных (автоматизированных) систем.

Учебные вопросы:

1. Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи.
2. Методы построения защищённых АС. Два основных метода проектирования. Метод проектирования «снизу вверх». Недостатки метода проектирования «снизу вверх».
3. Иерархический метод построения защищённой АС («сверху вниз»).
4. Принципы проектирования. Структурный принцип и принцип модульного проектирования.
5. Три основных конструкции для проектирования. Использование элемента DO-WHILE для организации цикла. Конструкция принятия двоичного решения IF-THEN-ELSE. Преимущества использования модульного принципа.
6. Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта.
7. Спецификация требований программного обеспечения. Функциональные критерии и характеристики. Неформализованные представления разработчика. Спецификация требований программного обеспечения (Software Requirements Specification).
8. Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной спецификации. Основные подходы к определению спецификаций требований.

9. Теория безопасных систем (ТСВ). Понятие «доверенная вычислительная среда» (trusted computing base-TCB).

10. Дискретная природа характеристики «безопасный». Характеристика «доверенный». Доверенная вычислительная среда. Набор компонентов, составляющий доверенную вычислительную среду.

11. Этапы разработки защищённой автоматизированной системы (АСЗИ). Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2014). Цель создания АСЗИ.

Продолжительность занятия — 2/1 часа.

3. Указания по проведению лабораторных работ

Лабораторная работа 1.

Тема: Общие сведения о системах передачи информации. Введение в теорию сигналов и систем.

Цель занятия: ознакомиться с общими сведениями о системах передачи информации.

Продолжительность занятия – 2/2 ч.

Задание:

1. Изучить общие сведения о системах передачи информации.
2. Определить роль и место теории сигналов и систем в современном обществе.
3. Оформить отчет по проведенному исследованию.

Лабораторная работа 2.

Тема: Кодирование источников сообщений и каналов связи. Методы модуляции.

Цель занятия: ознакомиться с устройством кодирования источников сообщений и каналов связи и методами модуляции.

Продолжительность занятия – 2/2 ч.

Задание:

1. Изучить основные принципы функционирования устройства кодирования источников сообщений и каналов связи.
2. Ознакомиться и охарактеризовать методы модуляции, выявить их достоинства и недостатки.
3. Оформить отчет по проведенному исследованию.

Лабораторная работа 3.

Тема: Принципы построения сетей связи. Основные характеристики сетей связи.

Цель занятия: ознакомиться с основными характеристиками и принципами построения сетей связи.

Продолжительность занятия – 4/2 ч.

Задание:

1. Изучить основные характеристики сетей связи.

2. Выявить базовые принципы функционирования сетей связи.
3. Оформить отчет по проведенному исследованию.

Лабораторная работа 4.

Тема: Многоканальные системы связи. Принципы построения систем радиосвязи.

Цель занятия: Дать характеристику многоканальных систем связи и выявить основные особенности построения систем радиосвязи.

Продолжительность занятия – 4/3 ч.

Задание:

1. Изучить и охарактеризовать многоканальные системы связи.
2. Определить основные особенности построения систем радиосвязи.
3. Оформить отчет по проведенному исследованию.

Лабораторная работа 5.

Тема: Особенности построения информационно-вычислительных систем.

Цель занятия: ознакомиться с базовыми принципами построения информационно-вычислительных систем.

Продолжительность занятия – 4/3 ч.

Задание:

1. Изучить базовые принципы построения информационно-вычислительных систем.
2. Выявить достоинства и недостатки существующих принципов построения информационно-вычислительных систем.
3. Оформить отчет по проведенному исследованию.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1	Актуальность проблемы обеспечения информационной безопасности для создаваемых защищенных информационных систем	Подготовка рефератов, письменная работа, самостоятельное изучение тем. Примерная тематика рефератов (докладов, письменных работ и т.д.): 1. Место информационной безопасности в системе национальной безопасности. 2. Современная концепция информационной безопасности. 3. Цели и концептуальные основы защиты информации. 4. Проблематика защиты информации в АСЗИ. 5. Проблематика защиты информации в ИСПДн. 6. Проблематика защиты информации в АСУ ТП КВО (КСИИ). 7. Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и

		функционального назначения. 8. Классификация АС по уровню защищённости от НСД к информации. 9. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации. 10. Классификация МЭ по уровню защищённости от НСД к информации.
2	Основные угрозы и уязвимости информационных систем, возможные атаки на них	Подготовка рефератов, письменная работа, самостоятельное изучение тем, создание презентаций. Примерная тематика рефератов (докладов, письменных работ и т.д.): 1. Виды и анализ угроз автоматизированных систем. 2. Компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников. 3. Базовая модель угроз ИСПДн. 4. Уязвимости АС, возможные атаки на них. 5. Модели нарушителей объектов защиты информации.
3	Комплексное обеспечение информационной безопасности информационных систем. Способы атак на уровне приложений и меры по снижению их уязвимости	Подготовка рефератов, письменная работа, самостоятельное изучение тем. Примерная тематика рефератов (докладов, письменных работ и т.д.): 1. Требования по защите информации в АС различных классов. 2. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС. 3. Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. 4. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков. **5.** Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи.
4	Методология формирования задач защиты для объектов информатизации, интеграция средств информационной безопасности в единую технологическую	Подготовка рефератов, письменная работа, самостоятельное изучение тем, создание презентаций. Примерная тематика рефератов (докладов, письменных работ и т.д.): 1. Задачи аттестации объектов информатизации в соответствии с нормативно-методическими документами. 2. Аттестация АС по требованиям безопасности информации. 3. Аттестация ЗП по требованиям безопасности информации. 4. Описание систем защиты с помощью матрицы доступа.

	среду построения защищенной ИС	Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU). 5. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant. 6. Три основных конструкции для проектирования. Использование элемента DO-WHILE для организации цикла. Конструкция принятия двоичного решения IF-THEN-ELSE. Преимущества использования модульного принципа.
5	Проектирование комплексной системы защиты информации (КСЗИ) в ИС	Подготовка рефератов, письменная работа, самостоятельное изучение тем, создание презентаций. Примерная тематика рефератов (докладов, письменных работ и т.д.): 1. Комплексные системы защиты информации. 2. Методы построения защищённых АС. Принципы проектирования. 3. Структурный принцип и принцип модульного проектирования защищённых АС. Преимущества использования модульного принципа. 4. Три основных конструкции для проектирования защищённых АС. 5. Этапы разработки защищённой автоматизированной системы (АСЗИ). Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2014). Цель создания АСЗИ.
6	Типовая структура КСЗИ от несанкционированного доступа (НСД) в ИС. Концептуальные положения системы менеджмента информационной безопасности применительно к ИС	Подготовка рефератов, письменная работа, самостоятельное изучение тем, создание презентаций. Примерная тематика рефератов (докладов, письменных работ и т.д.): 1. Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД. 2. Построение модели нарушителя безопасности АС. 3. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ. 4. Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта. 5. Спецификация требований программного обеспечения. Функциональные критерии и характеристики. Неформализованные представления разработчика. Спецификация требований программного обеспечения (Software Requirements Specification).
7	Методы и методики оценки качества (эффективности) ИБ при создании	Подготовка рефератов, письменная работа, самостоятельное изучение тем, создание презентаций. Примерная тематика рефератов (докладов, письменных работ и т.д.): 1. Оценка эффективности защиты информации на

	защищенных ИС	объектах информатизации. 2. Перечень основных документов ФСТЭК России по вопросам защиты информации. 3. Лицензирование и сертификация в области защиты информации.

5. Указания по проведению контрольных работ для студентов

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы «раскрыть», «определить», «установить», «показать», «выявить» и т.д.
3. Основная часть работы включает 2-4 вопроса, каждый из которых посвящается решению задач, сформированных во введении, и заканчивается констатацией итогов.
4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).
5. Необходимо давать ссылки на используемую литературу.
6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
7. Вслед за заключением идет список литературы, который должен быть составлен и оформлен с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

5.4. Примерная тематика контрольных работ:

1. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности. Основы обеспечения безопасности информации в компьютерных системах.
2. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.

3. Проектирование архитектуры системы защиты информации выбранного объекта и оценка его уровня защищённости.

4. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.

5. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации.

6. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию.

7. Направления повышения эффективности существующей системы защиты и методика применения средств защиты информации на выбранных объектах исследования.

8. Разработка проекта создания системы защиты информации на выбранных типовых офисных объектах.

9. Основные виды атак на компьютерные системы (КС), их классификация, проблемы обеспечения информационной безопасности в проводных КС.

10. Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.

11. Компьютерная преступность в экономических областях.

12. Компьютерные вирусы в современных информационных системах.

13. Информационные угрозы современным экономическим объектам.

14. Безопасность информации в коммерческой деятельности.

15. Становление и развитие промышленного шпионажа.

16. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.

17. Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU).

18. Направления повышения эффективности существующей системы защиты и методика применения средств защиты информации на выбранных объектах исследования.

19. Общий подход к построению систем, реализующих мандатную (полномочную) политику безопасности в модели BL (Белла-Лападулы).

20. Назначение модели Белла-Лападулы. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1.Антонов, Д. А. Применение коммутаторов в современных сетях передачи информации : учебно-методическое пособие / Д. А. Антонов, А. Е. Ермакова,

С. Е. Иконников. — Москва : РУТ (МИИТ), 2021. — 94 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/269750 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.
2.Лебедько, Е. Г. Теоретические основы передачи информации : монография / Е. Г. Лебедько. — Санкт-Петербург : Лань, 2022. — 352 с. — ISBN 978-5-8114-1139-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/210620 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

3.Зверева, Е. Н. Сборник примеров и задач по основам теории информации и кодирования сообщений : учебно-методическое пособие / Е. Н. Зверева, Е. Г. Лебедько. — Санкт-Петербург : НИУ ИТМО, 2014. — 76 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/71068 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.
4.Устиновский, Е. П. Проектирование цепных передач с применением ЭВМ : учебное пособие / Е. П. Устиновский, Е. В. Вайчулис, А. В. Ковнацкий. — Челябинск : ЮУрГУ, 2017. — 132 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167542 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
2. http://informika.ru/ – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. http://www.academy.it.ru/ – академия АЙТИ.
7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации.
9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
10. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

Перечень программного обеспечения: *MSOffice, Multisim.*
Информационные справочные системы:
Ресурсы информационно-образовательной среды МГОТУ:
Рабочая программа и методическое обеспечение по курсу «Сети и системы передачи информации»