МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования «Кабардино-Балкарский государственный университет
им. Х.М. Бербекова» (КБГУ)

ИНСТИТУТ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ЦИФРОВЫХ ТЕХНОЛОГИЙ

КАФЕДРА КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СОГЛАСОВАНО

Руководитель образовательной программы
_____А.С. Ксенофонтов

«30» 08 2022 г.

УТВЕРЖДАЮ

Директор ИИИиЦТ
_____ А.Х. Шапсигов

«30» 08 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ»

Направление подготовки (специальность)
10.03.01 – Информационная безопасность

Профиль подготовки:
«Организация и технология защиты информации»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
очная

Нальчик 2022

Рабочая программа дисциплины «Защита информации от утечки по техническим каналам» /сост. А.С. Ксенофонтов – Нальчик: ФГБОУ КБГУ, 2022. – 24 с.

Рабочая программа предназначена для преподавания дисциплины вариативной части студентам очной формы обучения по направлению подготовки 10.03.01 Информационная безопасность в 7 семестре.

Рабочая программа составлена с учетом Федерального государственного образовательного стандарта высшего образования по направлениям подготовки 10.03.01 Информационная безопасность, утвержденному приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. N 1427, зарегистрированного в Минюсте России 18 февраля 2021 г. N 62548.

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Целью дисциплины является раскрыть слушателям современное представление о видах, источниках и носителях защищаемой информации, дать классификацию и основные характеристики технических каналов утечки информации и методов технической защиты информации, представить государственную систему противодействия технической разведке, виды контроля эффективности защиты информации.

Основные задачи дисциплины:

- привести анализ физических процессов приводящих к появлению опасных сигналов, демаскирующих защищаемые объекты;
- дать физические основы процессов образования технических каналов утечки информации;
- дать физическое обоснование технических характеристик каналов утечки информации;
- изложить концепцию и методы инженерно-технической защиты информации;
- дать представление о формировании базы нормативных документов по противодействию технической и видам контроля эффективности защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП ВО

Дисциплина включена в вариативную часть обязательных дисциплин учебного плана по направлению подготовки ВО 10.03.01 Информационная безопасность профиль: Организация и технология защиты информации.

Изучение её базируется на следующих дисциплинах: «Физика», «Матанализ», «Дискретная математика».

Дисциплина «Защита информации от утечки по техническим каналам» является дисциплиной профессионального цикла и является опорой для дисциплины «Инженерно-техническая защита информации».

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки:

а) общепрофессиональные (ОПК):

способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ОПК-6);

способен использовать системы криптографической защиты информации в автоматизированных системах (ОПК-9.3);

б) Выпускник должен обладать следующими профессиональными компетенциями (ПКС):

Способен анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей (ПКС 5.2).

В результате изучения содержания курса студенты (слушатели) должны

Знать:

- цели, задачи, принципы и основные направления обеспечения информационной безопасности предприятия, угрозы предприятия на основе

анализа структуры и содержания информационных процессов его, угрозы информационной безопасности государства, содержание информационной войны, методы и средства ее ведения, понимать угрозы безопасности информации, методы анализа структуры и особенности функционирования объекта защиты, принципы организации информационных систем в соответствии с требованиями по защите информации

- правовые аспекты использование СВК, принципы построения СВК, основные структуры и схемотехнику элементов СВК, физические возможности каналов передачи данных СВК, основы схемотехники и элементную базу аналоговых и цифровых электронных устройств, а также архитектуру, положения и инструкции по оформлению технической документации, как произвести даунгрейд ПО программных и программно-аппаратных средств защиты информации;
- - основные криптографические методы и алгоритмы, используемые в программных, программно-аппаратных и технических средствах защиты информации, основные принципы построения криптоалгоритмов для настройки и обслуживания программно-аппаратных и технических средств, технические средства защиты информации.
- методы обработки экспериментальных данных при исследовании систем защиты информации, основные принципы, методы и средства измерений, использующиеся в проведении экспериментальных исследований системы защиты информации, активные и неактивные способы и средства скрытия информации;
- способы и средства технической дезинформации, условия и способы использования микропроцессоров и микропроцессорных систем в радиоэлектронных устройствах.

Уметь:

- проводить эксперименты по заданной методике, обработку экспериментальных данных, оценку погрешности и достоверности их результатов, применять полученные знания при проведении экспериментальных исследований системы защиты информации, обеспечивать выбор оптимальных (по условиям эксплуатации и экономичности) технических средств защиты информации, использовать стандартные пакеты прикладных программ для решения практических задач, применять действующие стандарты.
- реализовывать алгоритмы типовых задач обеспечения информационной безопасности; составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности, проводить анализ предметной области, сочетать элементы системы, проводить экспертную оценку объектов защиты, настраивать комплекс элементов, быстро разобраться в документации к программным, программно-аппаратным и техническим средствам защиты информации
- - «на месте» произвести апгрейд основных программных модулей программных, программно-аппаратных и технических средств защиты информации, строить и изучать математические модели конкретных явлений и процессов для решения принципиальных задач по обеспечению информационной безопасности программно-аппаратных (в том числе криптографических) и технических средств, использовать компьютеры и аппаратные средства вычислительной техники в средствах защиты информации, выполнять работы по установке, настройке и обслуживанию средств защиты информации.
- применять современные подходы к построению систем защиты информации, выбирать и анализировать показатели качества и критерии оценки систем

информационного нападения и систем защиты информации, определять информационные ресурсы, подлежащие защите, проводить классификацию объектов и субъектов информационных систем.

Владеть:

- навыками формальной постановки и решения задачи обеспечения информационной безопасности, навыками определения возможных путей нейтрализации угроз безопасности, принципами распределения прав и ответственности при организации доступа к объектам
- способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;
- способностью составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности, навыками работы с инструментальными средствами моделирования предметной области, прикладных процессов; навыками использования функциональных и технологических стандартов СВК; работы с инструментальными средствами проектирования СВК, методами, необходимыми для выбора элементной базы и конструкторских решений с учетом требований надежности, устойчивости к воздействию окружающей среды, электромагнитной совместимости и технологичности, навыками по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации, способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации борьбы с угрозами, на основе анализа структуры и содержания информационных процессов, целей и задач деятельности программно-аппаратных и технических средств, методами установки, настройки и обслуживанию средств защиты информации.
- навыками по использованию компьютерных программ и сетевых технологий по обработке экспериментальных данных, навыками использования радиоизмерительной техники в системах защиты информации, навыками практической эксплуатации современных технических средств защиты информации, навыками работы с информационными системами.

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ (МОДУЛЯ)

В таблице 1 приводится описание содержания дисциплины, структурированное по разделам, с указанием по каждому разделу формы текущего контроля: защита лабораторной работы (ЛР), коллоквиум (К), рубежный контроль (РК), тестирование (Т).

Таблица 1

№	Наименование раздела	Содержание раздела	Код контролируемой компетенции (или ее части)	Форма текущего контроля
1	Раздел 1. Виды, источники и носители защищаемой информации.	Демаскирующие признаки объектов наблюдения и сигналов. Опасные сигналы и их источники. Физические процессы, приводящие к появлению побочных излучений и формированию технических каналов утечки информации. Классификация и основные технические характеристики каналов утечки информации. Побочные электромагнитные	ОПК-6, ПКС 5.2	(К), (РК), (Т), (ЛР)

		излучения (ПЭМИ). Источники ПЭМИ. Формирование канала утечки информации по ПЭМИ. Приземный канал распространения ПЭМИ. Ослабление ПЭМИ при распространении вдоль земной поверхности. Приём и измерение ПЭМИ. Расчёт уровней опасных сигналов ПЭМИ. Расчет контролируемых зон по измеренному уровню сигналов ПЭМИ. Побочные каналы утечки информации за счёт наводок. Формирование каналов утечки информации за счёт наводок на посторонние проводники, случайные антенны, цепи питания и заземления. Расчет уровней опасных сигналов в каналах ПЭМИН. Основные характеристики технических каналов утечки информации образованных за счёт наводок. Акустический и вибрационный каналы утечки информации. Физические процессы, приводящие к появлению опасных акустических и вибрационных сигналов. Характеристики побочных акустических и вибрационных сигналов. Характеристики акустических и вибрационных каналов утечки информации. Расчёт уровней опасных сигналов ПАИ. Расчёт контролируемой зоны по уровню ПАИ.		
2	Раздел 2. Концепция и метод инженерно-технической защиты информации.	Классификация технической разведки. Возможности видов технической разведки. Структура и основные характеристики технических каналов утечки информации. Комплексирование при извлечении информации в каналах разведки. Методы и средства инженерной защиты и технической охраны объектов. Скрытие объектов наблюдения. Скрытие речевой информации в каналах связи. Энергетическое скрытие акустических информационных сигналов. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование информационных полей. Подавление информационных сигналов в цепях электропитания и заземления. Обнаружение и локализация закладных устройств. Методы поиска закладных устройств. Использование эффекта нелинейного рассеяния ЭМ для обнаружения и локализации закладных устройств.	ОПК-9.3, ПКС 5.2	(К), (РК), (Т), (ЛР)
3	Раздел 3. Характеристика	Нормативные документы по противодействию технической разведке.	ОПК-6	(К), (РК), (Т), (ЛР)

	государственной системы противодействия технической разведке.	Документы, регламентирующие требования к средствам защиты информации от утечки по техническим каналам, включая средства контроля эффективности защиты информации. Виды контроля эффективности защиты информации. Основные положения методологии инженерно-технической защиты информации. Нормирование уровней побочных излучений в целях защиты информации. Нормирование уровней побочных излучений по критерию информационной безопасности. Расчёт предельно допустимых отношений опасный сигнал/ шум в технических каналах утечки информации. Методы расчёта и инструментального контроля показателей защиты информации.		

5. *Структура дисциплины (модуля)*

Таблица 2. Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов).

Вид работы	**Трудоемкость, часы**	
	7 семестр	Всего
Общая трудоемкость (в часах)	**108**	**108**
Контактная работа (в часах):	**42**	**42**
Лекции (Л)	28	28
Лабораторные работы (ЛР)	28	28
Практические занятия (ПЗ)	14	14
Самостоятельная работа (в часах):	**29**	**29**
Курсовой проект (КП) Курсовая работа (КР)		
Самостоятельное изучение разделов	29	29
Подготовка и прохождение промежуточной аттестации	**9**	**9**
Вид промежуточной аттестации	**Зачет**	**Зачет**

Таблица 3. Лекционные занятия

№ п/п	**Тема**
1.	Физические процессы, приводящие к появлению побочных излучений и формированию технических каналов утечки информации. Классификация и основные технические характеристики каналов утечки информации.
2.	Побочные электромагнитные излучения (ПЭМИ). Источники ПЭМИ. Формирование канала утечки информации по ПЭМИ. Приземный канал распространения ПЭМИ. Ослабление ПЭМИ при распространении вдоль земной поверхности. Приём и измерение ПЭМИ. Расчёт уровней опасных сигналов ПЭМИ. Расчет контролируемых зон по измеренному уровню сигналов ПЭМИ.
3.	Побочные каналы утечки информации за счёт наводок. Расчет уровней опасных сигналов в каналах ПЭМИН.

4.	Физические процессы, приводящие к появлению опасных акустических и вибрационных сигналов. Характеристики побочных акустических и вибрационных сигналов.
5.	Расчёт уровней опасных сигналов ПАИ. Расчёт контролируемой зоны по уровню ПАИ.
6.	Классификация технической разведки. Структура и основные характеристики технических каналов утечки информации. Комплексирование при извлечении информации в каналах разведки.
7.	Методы и средства инженерной защиты и технической охраны объектов.
8.	Энергетическое скрытие акустических информационных сигналов. Экранирование информационных полей. Подавление информационных сигналов в цепях электропитания и заземления.
9.	Методы поиска закладных устройств. Использование эффекта нелинейного рассеяния ЭМ для обнаружения и локализации закладных устройств.
10.	Нормативные документы по противодействию технической разведке. Документы, регламентирующие требования к средствам защиты информации от утечки по техническим каналам, включая средства контроля эффективности защиты информации. Виды контроля эффективности защиты информации.
11.	Нормирование уровней побочных излучений в целях защиты информации. Нормирование уровней побочных излучений по критерию информационной безопасности.
12.	Методы расчёта и инструментального контроля показателей защиты информации.

Таблица 4. Лабораторные работы

№ ЛР	Наименование лабораторных работ
1	2
1	Формирование каналов утечки информации за счёт наводок на посторонние проводники, случайные антенны, цепи питания и заземления.
2	Акустический и вибрационный каналы утечки информации.
3	Скрытие объектов наблюдения. Скрытие речевой информации в каналах связи.
4	Подавление опасных сигналов акустоэлектрических преобразователей.
5	Обнаружение и локализация закладных устройств.

Таблица 5. Самостоятельное изучение разделов дисциплины

№ раздела	**Вопросы, выносимые на самостоятельное изучение**
1.	Демаскирующие признаки объектов наблюдения и сигналов. Опасные сигналы и их источники.
2.	Основные характеристики технических каналов утечки информации образованных за счёт наводок.
3.	Характеристики акустических и вибрационных каналов утечки информации.
4.	Возможности видов технической разведки.
5.	Основные положения методологии инженерно-технической защиты информации.
6.	Расчёт предельно допустимых отношений опасный сигнал/ шум в технических каналах утечки информации.

6. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО И РУБЕЖНОГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Примерный перечень вопросов на коллоквиум по темам дисциплины (модуля)

1. Технические каналы утечки информации. Классификация.
2. Цели и задачи инженерно-технической защиты информации
3. Угрозы безопасности информации
4. Коммерческая разведка. Промышленный шпионаж
5. ТСПИ и ВТСС
6. Электромагнитный канал утечки информации
7. Электрический канал утечки информации
8. Параметрический канал утечки информации
9. Акустический канал утечки информации
10. Вибрационный канал утечки информации
11. Визуальный канал утечки информации
12. Цели канала утечки ПЭМИН
13. Источники и особенности ПЭМИН
14. Способы защиты информации от утечки через канал ПЭМИН
15. Активная радиотехническая маскировка
16. Электромагнитное экранирование помещений
17. Эффективность экранирования от ПЭМИН
18. Физические процессы при электромагнитном экранировании
19. Материалы, применяемые при экранировании от ПЭМИН
20. Способы экранирования от ПЭМИН
21. Акустические речевые сигналы. Особенности их восприятия
22. Фонемы, октавы и форманты в акустическом речевом сигнале
23. Разборчивость речи
24. Словесная, слоговая и другие виды разборчивости речи
25. Характеристики речевого сигнала
26. Обстоятельства, влияющие на разборчивость речи
27. Порядок расчёта словесной разборчивости
28. Наиболее опасные объекты с точки зрения акустической разведки
29. Средства перехвата акустической информации
30. Особенности использования виброакустического канала
31. Звукопоглощающие материалы и конструкции
32. Звукопоглощающие конструкции
33. Резонансные звукопоглотители
34. Виброизоляция
35. Особенности распространения звука на открытом пространстве
36. Влияние атмосферы и погодных условий на распространение звука.
37. Направленные микрофоны. Виды.
38. Характеристики направленных микрофонов
39. Трубчатый, щелевой направленный микрофон.
40. Направленный микрофон органного типа.

Образцы тестовых заданий

1. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется
    a) достоверной
    b) конфиденциальной

c) документированной
d) коммерческой тайной

2. По доступности информация классифицируется на
   a) открытую информацию и государственную тайну
   b) конфиденциальную информацию и информацию свободного доступа
   c) информацию с ограниченным доступом и общедоступную информацию
   d) виды информации, указанные в остальных пунктах
3. К конфиденциальной информации относятся документы, содержащие
   a) информацию о гражданах
   b) законодательные акты
   c) "ноу-хау"
   d) сведения о золотом запасе страны
4. Безопасность информации -
   a) процесс создания и использования в автоматизированных системах специальных механизмов, поддерживающих установленный статус ее защищенности
   b) поддержание на заданном уровне тех параметров находящейся в автоматизированной системе информации, которые характеризуют установленный статус ее хранения, обработки и использования
   c) события или действия, которые могут вызвать нарушение функционирования автоматизированной системы, связанное с уничтожением или несанкционированным использованием обрабатываемой в ней информации
   d) состояние защищенности информации хранимая и обрабатываемая в автоматизированной системе, от негативного воздействия на нее с точки зрения нарушения ее физической и логической целостности или несанкционированного доступа
5. Запрещено относить к информации ограниченного доступа
   a) информацию о чрезвычайных ситуациях
   b) информацию о деятельности органов государственной власти
   c) документы открытых архивов и библиотек
   d) все, перечисленное в остальных пунктах

Промежуточная аттестация

Примерный перечень вопросов к зачету

1. Концепция инженерно-технической защиты информации.
2. Характеристика инженерно-технической защиты информации как области информационной безопасности.
3. Основные проблемы инженерно-технической защиты информации.
4. Цели и задачи защиты информации.
5. Ресурсы, выделяемые на защиту информации.
6. Принципы защиты информации техническими средствами.
7. Функции ФСБ России в области защиты информации.
8. Функции ФСТЭК России в области защиты информации.
9. Теоретические основы инженерно-технической защиты информации.
10. Свойства информации, влияющие на ее безопасность.
11. Виды, источники и носители защищаемой информации.
12. Демаскирующие признаки объектов наблюдения, сигналов и веществ.
13. Понятие об опасном сигнале.
14. Основные и вспомогательные технические средства, и системы, их классификация и характеристика.

15. Опасные сигналы, образующиеся в результате акустоэлектрических преобразований.
16. Виды побочных опасных электромагнитных излучений.
17. Паразитные связи и наводки опасных сигналов.
18. Виды опасных сигналов в помещении.
19. Основные задачи и органы технической разведки. Принципы технической разведки.
20. Возможности видов технической разведки по добыванию разведывательной информации.
21. Понятие и особенности утечки информации.
22. Структура, классификация и основные характеристики технических каналов утечки информации.
23. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.
24. Пространственное, энергетическое и структурное скрытие информации и ее носителей.
25. Комплексное применение методов защиты.
26. Звукоизоляция и звукопоглощение.
27. Энергетическое скрытие радио и электрических сигналов.
28. Физические основы защиты информации.
29. Акустоэлектрические преобразования.
30. Источники побочных излучений и наводок.
31. Особенности распространения акустических сигналов в помещениях.
32. Распространение радиосигналов различных диапазонов в пространстве и направляющим линиям связи.
33. Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе.
34. Подавление опасных сигналов акустоэлектрических преобразователей.
35. Экранирование электрических, магнитных, и электромагнитных полей.
36. Организационные основы инженерно-технической зашиты информации.
37. Основные задачи, структура и характеристика государственной системы защиты информации.
38. Основные руководящие, нормативные и методические документы по защите информации.
39. Основные организационные и технические меры по защите информации.
40. Понятие объекта информатизации.
41. Классификация и категорирование объектов информатизации.
42. Аттестация объектов информатизации.
43. Лицензирование деятельности по защите информации.
44. Сертификация средств защиты информации.
45. Виды контроля эффективности инженерно-технической защиты информации.
46. Специальные проверки технических средств.
47. Подготовительный этап проведения специального обследования.
48. Этап проведения специального обследования.
49. Заключительный этап проведения специального обследования.
50. Методическое обеспечение инженерно-технической защиты информации.
51. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации.
52. Принципы моделирования объектов защиты.

Контроль курсовых работ

Курсовые работы не предусмотрены.

7. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И ОПЫТА ДЕЯТЕЛЬНОСТИ

7.1. оценка качества освоения дисциплины

Максимальная сумма (100 баллов), набираемая студентом по дисциплине включает две составляющие:

– *первая составляющая* – оценка регулярности, своевременности и качества выполнения студентом учебной работы по изучению дисциплины в течение периода изучения дисциплины (семестра, или нескольких семестров) (сумма – не более 70 баллов). Баллы, характеризующие успеваемость студента по дисциплине, набираются им в течение всего периода обучения за изучение отдельных тем и выполнение отдельных видов работ.

– *вторая составляющая* – оценка знаний студента по результатам промежуточной аттестации (не более 30 –баллов).

Критерием оценки уровня сформированности компетенций в рамках учебной дисциплины является зачет.

Общий балл текущего и рубежного контроля складывается из следующих составляющих приложение 2. В течение учебного процесса студент обязан отчитаться по теоретическому материалу и практическим занятиям: опросы, индивидуальные задания.

Целью промежуточных аттестаций по дисциплине является оценка качества освоения дисциплины обучающимися.

Критерии оценки качества освоения дисциплины

Оценка «зачтено»– от 61 до 100 баллов – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы. Все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному. На экзамене студент демонстрирует глубокие знания предусмотренного программой материала, умеет четко, лаконично и логически последовательно отвечать на поставленные вопросы.

Или теоретическое содержание курса освоено, необходимые практические навыки работы сформированы, выполненные учебные задания содержат незначительные ошибки. На экзамене студент демонстрирует твердое знания основного (программного) материала, умеет четко, грамотно, без существенных неточностей отвечать на поставленные вопросы.

Оценка «незачтено» – от 36 до 60 баллов – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к существенному повышению качества выполнения учебных заданий. На экзамене студент демонстрирует незнание значительной части программного материала, существенные ошибки в ответах на вопросы, неумение ориентироваться в материале, незнание основных понятий дисциплины.

Таблица 6. Результаты освоения учебной дисциплины, подлежащие проверке.

Результаты обучения (компетенции)	**Основные показатели оценки результатов обучения**	**Вид оценочного материала**
способен анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей	*Знать:* цели, задачи, принципы и основные направления обеспечения информационной безопасности предприятия, угрозы предприятия на основе анализа структуры и содержания информационных процессов его, угрозы информационной безопасности государства, содержание	Коллоквиум Выполнение и защита лабораторных работ Тестирование

(ПКС 5.2).	информационной войны, методы и средства ее ведения, понимать угрозы безопасности информации, методы анализа структуры и особенности функционирования объекта защиты, принципы организации информационных систем в соответствии с требованиями по защите информации *Уметь:* применять современные подходы к построению систем защиты информации, выбирать и анализировать показатели качества и критерии оценки систем информационного нападения и систем защиты информации, определять информационные ресурсы, подлежащие защите, проводить классификацию объектов и субъектов информационных систем. *Владеть*: навыками формальной постановки и решения задачи обеспечения информационной безопасности, навыками определения возможных путей нейтрализации угроз безопасности, принципами распределения прав и ответственности при организации доступа к объектам	
способен использовать системы криптографической защиты информации в автоматизированных системах (ОПК-9.3)	*Знать:* правовые аспекты использование СВК, принципы построения СВК, основные структуры и схемотехнику элементов СВК, физические возможности каналов передачи данных СВК, основы схемотехники и элементную базу аналоговых и цифровых электронных устройств, а также архитектуру, положения и инструкции по оформлению технической документации, как произвести даунгрейд ПО программных и программно-аппаратных средств защиты информации; - основные криптографические методы и алгоритмы, используемые в программных, программно-аппаратных и технических средствах защиты информации, основные принципы построения криптоалгоритмов для настройки и обслуживания программно-аппаратных и технических средств, технические средства защиты информации.	Коллоквиум Выполнение и защита лабораторных работ Тестирование

	Уметь: реализовывать алгоритмы типовых задач обеспечения информационной безопасности; составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности, проводить анализ предметной области, сочетать элементы системы, проводить экспертную оценку объектов защиты, настраивать комплекс элементов, быстро разобраться в документации к программным, программно-аппаратным и техническим средствам защиты информации - «на месте» произвести апгрейд основных программных модулей программных, программно-аппаратных и технических средств защиты информации, строить и изучать математические модели конкретных явлений и процессов для решения принципиальных задач по обеспечению информационной безопасности программно-аппаратных (в том числе криптографических) и технических средств, использовать компьютеры и аппаратные средства вычислительной техники в средствах защиты информации, выполнять работы по установке, настройке и обслуживанию средств защиты информации. *Владеть*: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности; способностью составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности, навыками работы с инструментальными средствами моделирования предметной области, прикладных процессов; навыками использования функциональных и технологических стандартов СВК; работы с инструментальными средствами проектирования СВК, методами, необходимыми для выбора элементной базы и конструкторских решений с учетом требований надежности, устойчивости к	

	воздействию окружающей среды, электромагнитной совместимости и технологичности, навыками по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации, способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации борьбы с угрозами, на основе анализа структуры и содержания информационных процессов, целей и задач деятельности программно-аппаратных и технических средств, методами установки, настройки и обслуживанию средств защиты информации.	
способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ОПК-6)	*Знать:* методы обработки экспериментальных данных при исследовании систем защиты информации, основные принципы, методы и средства измерений, использующиеся в проведении экспериментальных исследований системы защиты информации, активные и неактивные способы и средства скрытия информации; способы и средства технической дезинформации, условия и способы использования микропроцессоров и микропроцессорных систем в радиоэлектронных устройствах. *Уметь:* проводить эксперименты по заданной методике, обработку экспериментальных данных, оценку погрешности и достоверности их результатов, применять полученные знания при проведении экспериментальных исследований системы защиты информации, обеспечивать выбор оптимальных (по условиям эксплуатации и экономичности) технических средств защиты информации, использовать стандартные пакеты прикладных программ для решения практических задач, применять действующие стандарты. *Владеть*: навыками по использованию компьютерных программ и сетевых	Коллоквиум Выполнение и защита лабораторных работ Тестирование

	технологий по обработке экспериментальных данных, навыками использования радиоизмерительной техники в системах защиты информации, навыками практической эксплуатации современных технических средств защиты информации, навыками работы с информационными системами.	

7.2. *Основная литература*

1. Голиков А.М. Защита информации от утечки по техническим каналам [Электронный ресурс]: учебное пособие/ Голиков А.М.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2015.— 256 c.— Режим доступа: http://www.iprbookshop.ru/72090.html.— ЭБС «IPRbooks»
2. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 c.— Режим доступа: http://www.iprbookshop.ru/52161.html.— ЭБС «IPRbooks»
3. Джонс К.Д. Инструментальные средства обеспечения безопасности [Электронный ресурс]/ Джонс К.Д., Шема М., Джонсон Б.С.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 914 c.— Режим доступа: http://www.iprbookshop.ru/73679.html.— ЭБС «IPRbooks»

7.3. *Дополнительная литература*

1. Каторин Ю.Ф. Защита информации техническими средствами [Электронный ресурс]: учебное пособие/ Каторин Ю.Ф., Разумовский А.В., Спивак А.И.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2012.— 417 c.— Режим доступа: http://www.iprbookshop.ru/66445.html.— ЭБС «IPRbooks»
2. Креопалов В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие/ Креопалов В.В.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2011.— 278 c.— Режим доступа: http://www.iprbookshop.ru/10871.html.— ЭБС «IPRbooks»
3. Иванов А.В. Защита речевой информации от утечки по акустоэлектрическим каналам [Электронный ресурс]: учебное пособие/ Иванов А.В., Трушин В.А.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2012.— 43 c.— Режим доступа: http://www.iprbookshop.ru/44919.html.— ЭБС «IPRbooks»
4. Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 187 c.— Режим доступа: http://www.iprbookshop.ru/7000.html.— ЭБС «IPRbooks»

7.4. *Периодические издания*

Перечень периодических изданий, получаемых библиотекой КБГУ:

- Вестник МГУ. Вычислительная математика и кибернетика
- Вестник российского общества информатики и вычислительной техники

- Информатика и образование
- Информационные технологии
- Мир ПК
- Персональный компьютер сегодня
- Программирование
- Информационная безопасность

7.5. *Интернет-ресурсы*

1. http://fstec.ru/ Федеральная служба по техническому и экспортному контролю
2. http://www.fsb.ru/ Федеральная служба безопасности
3. http://clsz.fsb.ru/ Центр по лицензированию, сертификации и защите государственной тайны ФСБ России
4. http://pravo.gov.ru/ Официальный интернет-портал правовой информации

7.6. *Методические указания по проведению различных учебных занятий, к курсовому проектированию и другим видам самостоятельной работы*

Методические рекомендации при работе над конспектом во время проведения лекции

В процессе лекционных занятий целесообразно конспектировать учебный материал. Для этого используются общие и утвердившиеся в практике правила, и приемы конспектирования лекций:

Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Целесообразно записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.

Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их. В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.

Каждому студенту необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.

Методические рекомендации при подготовке к коллоквиуму

- проработать конспекты лекций по вопросам коллоквиума;
- прочитать основную и дополнительную литературу, рекомендованную по изучаемым вопросам;
- ответить на вопросы коллоквиума;
- при затруднениях, проконсультироваться с преподавателем.

Критерии оценивания

Оценка			
неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**

2 балла	4 балла	6 баллов	8 баллов
Студент не знает значительной части вопросов, допускает существенные ошибки в ответах на вопросы.	Студент поверхностно знает вопросы коллоквиума, допускает неточности в ответе на вопрос	Студент хорошо знает материал, грамотно и по существу излагает его, допуская некоторые неточности в ответе на вопрос.	Студент в полном объеме знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

Методические рекомендации по организации самостоятельной работы

Самостоятельная работа (по В.И. Далю «самостоятельный – человек, имеющий свои твердые убеждения») осуществляется при всех формах обучения: очной и заочной.

Самостоятельная работа обучающихся - способ активного, целенаправленного приобретения студентом новых для него знаний и умений без непосредственного участия в этом процесса преподавателей. Повышение роли самостоятельной работы обучающихся при проведении различных видов учебных занятий предполагает:

– оптимизацию методов обучения, внедрение в учебный процесс новых технологий обучения, повышающих производительность труда преподавателя, активное использование информационных технологий, позволяющих обучающемуся в удобное для него время осваивать учебный материал;

– широкое внедрение компьютеризированного тестирования;

– совершенствование методики проведения практик и научно-исследовательской работы обучающихся, поскольку именно эти виды учебной работы в первую очередь готовят обучающихся к самостоятельному выполнению профессиональных задач;

– модернизацию системы курсового и дипломного проектирования, которая должна повышать роль студента в подборе материала, поиске путей решения задач.

Самостоятельная работа приводит студента к получению нового знания, упорядочению и углублению имеющихся знаний, формированию у него профессиональных навыков и умений. Самостоятельная работа выполняет ряд функций:

– развивающую;
– информационно-обучающую;
– ориентирующую и стимулирующую;
– воспитывающую;
– исследовательскую.

В рамках курса выполняются следующие виды самостоятельной работы:

1. Проработка учебного материала (по конспектам, учебной и научной литературе);
2. Выполнение разноуровневых задач и заданий;
3. Работа с тестами и вопросами для самопроверки;
4. Выполнение итоговой контрольной работы.

Студентам рекомендуется с самого начала освоения курса работать с литературой и предлагаемыми заданиями в форме подготовки к очередному аудиторному занятию. При этом актуализируются имеющиеся знания, а также создается база для усвоения нового материала, возникают вопросы, ответы на которые студент получает в аудитории.

Необходимо отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику. При освоении курса студент может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой. Значительную помощь в подготовке к очередному занятию может оказать имеющийся в учебно-методическом комплексе краткий конспект лекций. Он же может использоваться и для закрепления полученного в аудитории материала. Самостоятельная работа студентов предусмотрена учебным планом и выполняется в обязательном порядке. Задания

предложены по каждой изучаемой теме и могут готовиться индивидуально или в группе. По необходимости студент может обращаться за консультацией к преподавателю. Выполнение заданий контролируется и оценивается преподавателем.

Для успешного самостоятельного изучения материала сегодня используются различные средства обучения, среди которых особое место занимают информационные технологии разного уровня и направленности: электронные учебники и курсы лекций, базы тестовых заданий и задач. Электронный учебник представляет собой программное средство, позволяющее представить для изучения теоретический материал, организовать апробирование, тренаж и самостоятельную творческую работу, помогающее студентам и преподавателю оценить уровень знаний в определенной тематике, а также содержащее необходимую справочную информацию. Электронный учебник может интегрировать в себе возможности различных педагогических программных средств: обучающих программ, справочников, учебных баз данных, тренажеров, контролирующих программ.

Для успешной организации самостоятельной работы все активнее применяются разнообразные образовательные ресурсы в сети Интернет: системы тестирования по различным областям, виртуальные лекции, лаборатории, при этом пользователю достаточно иметь компьютер и подключение к Интернету для того, чтобы связаться с преподавателем, решать вычислительные задачи и получать знания. Использование сетей усиливает роль самостоятельной работы студента и позволяет кардинальным образом изменить методику преподавания.

Студент может получать все задания и методические указания через сервер, что дает ему возможность привести в соответствие личные возможности с необходимыми для выполнения работ трудозатратами. Студент имеет возможность выполнять работу дома или в аудитории. Большое воспитательное и образовательное значение в самостоятельном учебном труде студента имеет самоконтроль. Самоконтроль возбуждает и поддерживает внимание и интерес, повышает активность памяти и мышления, позволяет студенту своевременно обнаружить и устранить допущенные ошибки и недостатки, объективно определить уровень своих знаний, практических умений. Самое доступное и простое средство самоконтроля с применением информационно-коммуникационных технологий - это ряд тестов «on-line», которые позволяют в режиме реального времени определить свой уровень владения предметным материалом, выявить свои ошибки и получить рекомендации по самосовершенствованию.

Методические рекомендации по работе с литературой

Всю литературу можно разделить на учебники и учебные пособия, оригинальные научные монографические источники, научные публикации в периодической печати. Из них можно выделить литературу основную (рекомендуемую), дополнительную и литературу для углубленного изучения дисциплины.

Изучение дисциплины следует начинать с учебника, поскольку учебник – это книга, в которой изложены основы научных знаний по определенному предмету в соответствии с целями и задачами обучения, установленными программой.

При работе с литературой необходимо учитывать, что имеются различные виды чтения, и каждый из них используется на определенных этапах освоения материала.

Предварительное чтение направлено на выявление в тексте незнакомых терминов и поиск их значения в справочной литературе. В частности, при чтении указанной литературы необходимо подробнейшим образом анализировать понятия.

Сквозное чтение предполагает прочтение материала от начала до конца. Сквозное чтение литературы из приведенного списка дает возможность студенту сформировать свод основных понятий из изучаемой области и свободно владеть ими.

Выборочное – наоборот, имеет целью поиск и отбор материала. В рамках данного курса выборочное чтение, как способ освоения содержания курса, должно использоваться при подготовке к практическим занятиям по соответствующим разделам.

Аналитическое чтение – это критический разбор текста с последующим его конспектированием. Освоение указанных понятий будет наиболее эффективным в том случае, если при чтении текстов студент будет задавать к этим текстам вопросы. Часть из этих вопросов сформулирована в ФОС в перечне вопросов для собеседования. Перечень этих вопросов ограничен, поэтому важно не только содержание вопросов, но сам принцип освоения литературы с помощью вопросов к текстам.

Целью *изучающего* чтения является глубокое и всестороннее понимание учебной информации. Есть несколько приемов изучающего чтения:

1. Чтение по алгоритму предполагает разбиение информации на блоки: название; автор; источник; основная идея текста; фактический материал; анализ текста путем сопоставления имеющихся точек зрения по рассматриваемым вопросам; новизна.
2. Прием постановки вопросов к тексту имеет следующий алгоритм:
   - медленно прочитать текст, стараясь понять смысл изложенного;
   - выделить ключевые слова в тексте;
   - постараться понять основные идеи, подтекст и общий замысел автора.
3. Прием тезирования заключается в формулировании тезисов в виде положений, утверждений, выводов.

К этому можно добавить и иные приемы: прием реферирования, прием комментирования.

Важной составляющей любого солидного научного издания является список литературы, на которую ссылается автор. При возникновении интереса к какой-то обсуждаемой в тексте проблеме всегда есть возможность обратиться к списку относящейся к ней литературы. В этом случае вся проблема как бы разбивается на составляющие части, каждая из которых может изучаться отдельно от других. При этом важно не терять из вида общий контекст и не погружаться чрезмерно в детали, потому что таким образом можно не увидеть главного.

Подготовка к экзамену должна проводиться на основе лекционного материала, материала практических занятий с обязательным обращением к основным учебникам по курсу. Это позволит исключить ошибки в понимании материала, облегчит его осмысление, прокомментирует материал многочисленными примерами.

Методические рекомендации по написанию рефератов

Реферат представляет собой сокращенный пересказ содержания первичного документа (или его части) с основными фактическими сведениями и выводами. Написание реферата используется в учебном процессе вуза в целях приобретения студентом необходимой профессиональной подготовки, развития умения и навыков самостоятельного научного поиска: изучения литературы по выбранной теме, анализа различных источников и точек зрения, обобщения материала, выделения главного, формулирования выводов и т. п. С помощью рефератов студент глубже постигает наиболее сложные проблемы курса, учится лаконично излагать свои мысли, правильно оформлять работу, докладывать результаты своего труда. Процесс написания реферата включает: выбор темы; подбор нормативных актов, специальной литературы и иных источников, их изучение; составление плана; написание текста работы и ее оформление; устное изложение реферата.

Рефераты пишутся по наиболее актуальным темам. В них на основе тщательного анализа и обобщения научного материала сопоставляются различные взгляды авторов и определяется собственная позиция студента с изложением соответствующих аргументов. Темы рефератов должны охватывать и дискуссионные вопросы курса. Они призваны отражать передовые научные идеи, обобщать тенденции практической деятельности, учитывая при этом изменения в текущем законодательстве. Рекомендованная ниже тематика рефератов примерная. Студент при желании может сам предложить ту или иную тему, предварительно согласовав ее с научным руководителем.

Реферат, как правило, состоит из введения, в котором кратко обосновывается актуальность, научная и практическая значимость избранной темы, основного материала,

содержащего суть проблемы и пути ее решения, и заключения, где формируются выводы, оценки, предложения. Общий объем реферата 20 листов.

Технические требования к оформлению реферата следующие. Реферат оформляется на листах формата А4, с обязательной нумерацией страниц, причем номер страницы на первом, титульном, листе не ставится. Поля: верхнее, нижнее, правое, левое – 20 мм. Абзацный отступ – 1,25; Рисунки должны создаваться в циклических редакторах или как рисунок Microsoft Word (сгруппированный). Таблицы выполнять табличными ячейками Microsoft Word. Сканирование рисунков и таблиц не допускается. Выравнивание текста (по ширине страницы) необходимо выполнять только стандартными способами, а не с помощью пробелов. Размер текста в рисунках и таблицах – 12 кегль. На титульном листе реферата нужно указать: название учебного заведения, факультета, номер группы и фамилию, имя и отчество автора, тему, место и год его написания. Рекомендуемый объем работы складывается из следующих составляющих: титульный лист (1 страница), содержание (1 страница), введение (1 – 2 страницы), основная часть, которую можно разделить на главы или разделы (10 – 15 страниц), заключение (1 – 3 страницы), список литературы (1 страница), приложение (не обязательно). Если реферат содержит таблицу, то ее номер и название располагаются сверху таблицы, если рисунок, то внизу рисунка.

Содержательные части реферата – это введение, основная часть и заключение. Введение должно содержать рассуждение по поводу того, что рассматриваемая тема актуальна (то есть современна и к ней есть большой интерес в настоящее время), а также постановку цели исследования, которая непосредственно связана с названием работы. Также во введении могут быть поставлены задачи (но не обязательно, так как работа невелика по объему), которые детализируют цель. В заключении пишутся конкретные, содержательные выводы.

Содержание реферата студент докладывает на семинаре, кружке, научной конференции. Предварительно подготовив тезисы доклада, студент в течение 7 - 10 минут должен кратко изложить основные положения своей работы. После доклада автор отвечает на вопросы, затем выступают оппоненты, которые заранее познакомились с текстом реферата, и отмечают его сильные и слабые стороны. На основе обсуждения обучающемуся выставляется соответствующая оценка.

Методические рекомендации по выполнению лабораторных работ

Выполнение каждой лабораторной работы складывается из следующих этапов.

1. Самостоятельная подготовка студентов к работе. Перед началом работы студенты должны четко представлять себе цель работы, изучить теоретические сведения к лабораторной работе

2. Выполнение работы. Этот этап осуществляется в соответствии с методическими указаниями, которые содержатся в описании к каждой работе. Сформулировать выводы по проделанной работе.

3. Составление отчета о проделанной работе. К отчету о выполненной работе предъявляются следующие требования:

Отчет должен содержать исчерпывающие данные, как о цели работы, так и о результатах в следующей последовательности:

- Титульный лист
- цель работы
- задание на лабораторную работу для своего варианта
- ответы на контрольные вопросы
- результаты выполнения работы
- выводы по работе.

4. Защита лабораторной работы с представлением отчета. Защита лабораторной работы проходит в форме свободной беседы по теме лабораторной работы.

Методические рекомендации по подготовке к тестированию

Тесты – это вопросы или задания, предусматривающие конкретный, краткий, четкий ответ на имеющиеся эталоны ответов. При самостоятельной подготовке к тестированию студенту необходимо:

а) готовясь к тестированию, проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;

б) четко выясните все условия тестирования заранее. Знать, сколько тестов Вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

в) приступая к работе с тестами, внимательно и до конца прочтите вопрос и предлагаемые варианты ответов. Выберите правильные (их может быть несколько). На отдельном листке ответов выпишите цифру вопроса и буквы, соответствующие правильным ответам;

г) в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.

д) если Вы встретили чрезвычайно трудный для Вас вопрос, не тратьте много времени на него. Переходите к другим тестам. Вернитесь к трудному вопросу в конце.

е) обязательно оставьте время для проверки ответов, чтобы избежать механических ошибок.

Критерии оценивания

Оценка			
неудовлетворительно 0 баллов	**удовлетворительно 3 балла**	**хорошо 4 балла**	**отлично 5 баллов**
Менее 50 % правильно выполненных заданий.	50-70% правильно выполненных заданий.	71-85% правильно выполненных заданий.	86-100% правильно выполненных заданий.

8. Материально-техническое обеспечение дисциплины

Программное обеспечение современных информационно-коммуникационных технологий

1. Студенты имеют доступ к единому образовательному порталу, где могут в открытом доступе пользоваться ресурсами учебно-методической литературы, являющимися разработками ведущих ВУЗОВ России.

2. Для рейтингового контроля используется система компьютерного тестирования на базе программного обеспечения Moodle.

3. Специализированная аудитория, используемая при проведении занятий лекционного типа №42, №58 оснащена мультимедийным проектором и комплектом аппаратуры, позволяющей демонстрировать текстовые и графические материалы.

Лаборатории оснащены необходимым оборудованием: Аппаратно-программный комплекс Sound Cleaner II, ЛГШ 701, АПК «Колибри», АПК «ST 131 Пиранья II», Microsoft Office, 7-zip, Adobe Acrobat Reader DC и др.

- Продукты MICROCOFT (WINEDUperDVC ALNG UpgrdSAPk MVL A Faculty EES (Корпоративная подписка на продукты Windows операционная система и офис)) ДОГОВОР №10/ЭА-223.

- Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 1500-2499 Node 1 year Educational Renewal License, ДОГОВОР № 15/ЭА-223.
- Mathlab/Simulink ДОГОВОР №80/ЕЛ-223.
- Adobe Creative Cloud for Teams – All Apps. Лицензии Education Device license для образовательных организаций ДОГОВОР № 15/ЭА-223.
- ABBYY FineReader ДОГОВОР № 15/ЭА-223.
- Антиплагиат ВУЗ ДОГОВОР № 15/ЭА-223.
- файловый менеджер Far Manager.
- 7zip-архиватор.
- Adobe Reader (свободное распространение)

Студенты имеют доступ через Интернет доступ к единому образовательному порталу, где в открытом доступе имеются ресурсы учебно-методической литературы, являющиеся разработками ведущих ВУЗов России.

8.1. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для студентов с ограниченными возможностями здоровья созданы специальные условия для получения образования. В целях доступности получения высшего образования по образовательным программам инвалидами и лицами с ограниченными возможностями здоровья университетом обеспечивается:

1. Альтернативная версия официального сайта в сети «Интернет» для слабовидящих;

2. Для инвалидов с нарушениями зрения (слабовидящие, слепые):

– присутствие ассистента, оказывающего обучающемуся необходимую помощь, дублирование вслух справочной информации о расписании учебных занятий; наличие средств для усиления остаточного зрения, брайлевской компьютерной техники, видеоувеличителей, программ невизуального доступа к информации, программ-синтезаторов речи и других технических средств приема-передачи учебной информации в доступных формах для студентов с нарушениями зрения;

– задания для выполнения на экзамене зачитываются ассистентом;

– письменные задания выполняются на бумаге, надиктовываются ассистенту обучающимся;

3.Для инвалидов и лиц с ограниченными возможностями здоровья по слуху (слабослышащие, глухие):

– на зачете/экзамене присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);

– зачет/экзамен проводится в письменной форме;

4. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, созданы материально-технические условия, обеспечивающие возможность беспрепятственного доступа обучающихся в учебные помещения, объекту питания, туалетные и другие помещения университета, а также пребывания в указанных помещениях (наличие расширенных дверных проемов, поручней и других приспособлений).

– письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

– по желанию студента экзамен проводится в устной форме.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

9. ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа:
одобрена на 2021/2022 учебный год. Протокол № ____ заседания кафедры от «___»_____20__ г.

В рабочую программу внесены следующие изменения:

_____
_____
_____
_____
_____

Разработчик программы _____
Зав. кафедрой _____

одобрена на 2022/2023 учебный год. Протокол № ____ заседания кафедры от «___»_____20__ г.

В рабочую программу внесены следующие изменения:

_____
_____
_____
_____
_____
_____

Разработчик программы _____
Зав. кафедрой _____

одобрена на 2023/2024 учебный год. Протокол № ____ заседания кафедры от «___»_____20__ г.

В рабочую программу внесены следующие изменения:

_____
_____
_____
_____
_____

Разработчик программы _____
Зав. кафедрой _____

ПРИЛОЖЕНИЕ

Распределение баллов текущего и рубежного контроля

№п/п	Вид контроля	Сумма баллов			
		Общая сумма	1-я точка	2-я точка	3-я точка
1	Посещение занятий	до 10 баллов	до 3 б.	до 3б.	до 4б.
2	Текущий контроль:	до 30 баллов	до 10 б.	до 10 б.	до 10 б.
3	Рубежный контроль (тестирование и коллоквиум)	до 30 баллов	до 10 б.	до 10 б.	до 10 б.
4	Итого сумма текущего и рубежного контроля	до 70 баллов	до 23б	до 23 б	до 24 б

Приложение 2

Распределение баллов текущего и рубежного контроля

№п/п	*Вид контроля*	*Сумма баллов*			
		Обшая сумма	*1-я точка*	*2-я точка*	*3-я точка*
1-	***Посещение занятий***	***до 10 баллов***	***до 3 б.***	***до 3б.***	***до 4б.***
2-	***Текущий контроль:***	***до 30 баллов***	***до 10 б.***	***до 10 б.***	***до 10 б.***
	Ответ на 5 вопросов	*от 0 до15 б.*	*от 0 до 5 б.*	*от0 до 5 б.*	*от0 до 5 б.*
	Полный правильный ответ	до 15 баллов	5 б.	5 б.	5 б.
	Неполный правильный ответ	от 3 до15 б.	от1 до 5 б.	от 1 до 5 б.	от 1 до 5 б.
	Ответ, содержащий неточности, ошибки	0б.	0б.	0б.	0б.
	Выполнение самостоятельных заданий (решение задач, написание рефератов, доклад, эссе)	*от 0 до15 б.*	*от 0 до 5 б.*	*от 0 до 5 б*	*от 0 до 5 б*
1.	***Рубежный контроль***	***до 30 баллов***	***до 10 б.***	***до 10 б.***	***до 10 б.***
	тестирование	от 0- до 12б.	от 0- до 4б.	от 0- до 4б.	от 0- до 4б.
	коллоквиум	от 0 до 18б.	от 0 до 6 б.	от 0 до 6 б.	от 0 до 6 б.
	Итого сумма текущего и рубежного контроля	***до 70баллов***	***до 23б.***	***до 23б***	***до 24б***
	Первый этап (базовый)уровень) – оценка «удовлетворительно»	не менее 36 б.	не менее 12 б.	не менее 12 б	не менее 12 б
	Второй этап (продвинутый)уровень) – оценка «хорошо»	менее 70 б. (51-69 б.)	менее 23 б	менее 23 б	менее 24б
	Третий этап (высокий уровень) - оценка «отлично»	не менее 70 б.	не менее 23 б.	не менее 23 б	не менее 24б