

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ «КАБАРДИНО-БАЛКАРСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ИМ. Х.М. БЕРБЕКОВА» (КБГУ)

ИНСТИТУТ ИНФОРМАТИКИ, ЭЛЕКТРОНИКИ И РОБОТОТЕХНИКИ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СОГЛАСОВАНО

УТВЕРЖДАЮ

Руководитель образовательной программы

Директора ИИЭР

_____ А.С. Ксенофонов

_____ Н.В. Черкесова

«___» _____ 2019 г.

«___» _____ 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Техническая защита информации

Направление подготовки

10.03.01 - Информационная безопасность

Профиль подготовки

Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника

Бакалавр

Форма обучения

Очная

Нальчик 2019

Рабочая программа дисциплины «Техническая защита информации» / сост. ст. преподаватель Арванова С.М. – Нальчик: ФГБОУ КБГУ, 2019. – 27 с.

Рабочая программа предназначена для преподавания дисциплины вариативной части студентам очной формы обучения по направлению подготовки 10.03.01 Информационная безопасность, в 7 семестре, 4 курса.

Рабочая программа составлена с учетом федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, зарегистрировано в Министерстве юстиции РФ № 1515 от 01.12.2016.

СОДЕРЖАНИЕ

| | |
|---|----|
| 1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ | 4 |
| 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО | 4 |
| 3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ..... | 4 |
| 4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ | 6 |
| 5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО И РУБЕЖНОГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ | 9 |
| Примерный перечень вопросов на коллоквиум по темам дисциплины..... | 11 |
| 6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ..... | 15 |
| 7. Учебно-методическое обеспечение дисциплины | 19 |
| 7.1. Нормативно-правовая база..... | 19 |
| 7.2. Основная литература | 19 |
| 7.3. Дополнительная литература | 19 |
| 7.4. Периодические издания (газета, вестник, бюллетень, журнал) | 20 |
| 7.5. Интернет-ресурсы | 20 |
| 7.6. Современные профессиональные базы данных..... | 20 |
| 7.7. Методические указания по проведению различных учебных занятий, к курсовому проектированию и другим видам самостоятельной работы | 20 |
| 8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ..... | 24 |
| 8.1. Требования к материально-техническому обеспечению | 24 |

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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 В СТРУКТУРЕ ОПОП ВО

Дисциплина включена в вариативную часть обязательных дисциплин учебного плана по направлению подготовки ВО 10.03.01 Информационная безопасность профиль: Информационно-аналитические системы финансового мониторинга.

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

Дисциплина «Техническая защита информации» является дисциплиной профессионального цикла и является опорой для дисциплины «Инженерно-техническая защита информации».

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

а) общепрофессиональные (ОПК):

способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7);

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

способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);

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 разбираться 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

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 | ОПК-7 ПК-1 | (К), (РК), (Т), (ЛР) |

| | | | | |
|---|--|--|------------------------|-------------------------|
| | | <p>утечки информации. 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. 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.</p> | | |
| 2 | Раздел 2. Концепция и метод инженерно-технической защиты информации. | <p>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 скрывание 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.</p> | ОПК-7 ПК-1 ПК-12 | (К), (ПК), (Т), (ЛР) |
| 3 | Раздел 3. Характеристика государственной системы противодействия технической разведке. | <p>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. 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.</p> | ПК-1 ПК-12 | (К), (ПК), (Т), (ЛР) |

Структура дисциплины

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 |
| <i>Лекции (Л)</i> | 14 | 14 |
| <i>Лабораторные работы (ЛР)</i> | 14 | 14 |
| <i>Практические занятия (ПЗ)</i> | 14 | 14 |
| Самостоятельная работа (в часах): | 66 | 66 |
| Курсовой проект (КП) | | |
| Курсовая работа (КР) | | |
| Самостоятельное изучение разделов | 66 | 66 |
| Подготовка и прохождение промежуточной аттестации | | |
| 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 скрывание 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. |

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

Формы контроля текущих, рубежных и промежуточных знаний студентов по дисциплине определяются в соответствии с учебным планом образовательной программы и в соответствии с действующим Положением о балльно-рейтинговой системе оценки успеваемости студентов КБГУ.

От обучающихся требуется посещение занятий, выполнение лабораторных работ, знакомство с рекомендованной литературой.

При аттестации обучающихся оценивается качество работы на занятиях (умение вести дискуссию, способность четко и ёмко формулировать свои мысли), уровень подготовки к самостоятельной деятельности, качество выполнения заданий (презентаций, докладов, выполнение лабораторных работ и др.).

Конечными результатами освоения программы дисциплины являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего семестра по этапам в рамках различного вида занятий и самостоятельной работы.

5.1. Оценочные материалы для текущего контроля.

Цель текущего контроля – оценка результатов работы в семестре и обеспечение своевременной обратной связи, для коррекции обучения, активизации самостоятельной

работы обучающегося. Объектом текущего контроля являются конкретизированные результаты обучения (учебные достижения) по дисциплине.

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины, оценка качества подготовки на основании выполненных заданий ведется преподавателем (с обсуждением результатов), баллы.

Критерии формирования оценок (оценивания) устного опроса

Устный опрос является одним из основных способов учёта знаний обучающегося по дисциплине. Развёрнутый ответ должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения.

В результате устного опроса знания, обучающегося оцениваются по следующей шкале:

| 3 балла | 2 балла | 1 балл | 0 баллов |
|---|--|---|--|
| ставится, если обучающийся: 1) полно излагает изученный материал, даёт правильное определенное экономических понятий; 2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные; 3) излагает материал последовательно и правильно с точки зрения норм литературного языка. | ставится, если обучающийся даёт ответ, удовлетворяющий тем же требованиям, что и для балла «1», но допускает 1-2 ошибки, которые сам же исправляет, и 1-2 недочёта в последовательности и языковом оформлении излагаемого. | ставится, если обучающийся обнаруживает знание и понимание основных положений данной темы, но: 1) излагает материал неполно и допускает неточности в определении понятий; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого. | ставится, если обучающийся обнаруживает незнание большей части соответствующего раздела изучаемого материала, допускает ошибки в формулировке. |

Баллы «1», «2», «3» могут ставиться не только за единовременный ответ, но и за рассредоточенный во времени, т.е. за сумму ответов, данных на протяжении занятия. начисляются в зависимости от сложности задания.

5.2. Оценочные материалы для самостоятельной работы обучающегося (типовые задачи) (при наличии)

Рабочая программа предусматривает проведение лекционных, лабораторных занятий, а также самостоятельную работу обучающихся. В ФГБОУ ВО «Кабардино-Балкарский государственный университет» действует балльно-рейтинговая система оценки учебных достижений, обучающихся по образовательным программам, реализуемым на основании федеральных государственных образовательных стандартов. Балльно-рейтинговая система

оценки знаний является одной из составляющих системы управления качеством образовательной деятельности в университете.

Примерный перечень вопросов на коллоквиум по темам дисциплины

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. Трубочатый, щелевой направленный микрофон.
40. Направленный микрофон органного типа.

Образцы тестовых заданий

1. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется
 - : достоверной
 - : конфиденциальной

- + : документированной
- : коммерческой тайной
- 2. По доступности информация классифицируется на
 - : открытую информацию и государственную тайну
 - : конфиденциальную информацию и информацию свободного доступа
 - + : информацию с ограниченным доступом и общедоступную информацию
 - : 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 хранящаяся 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

Примерный перечень вопросов к зачету (ОПК-7, ПК-1, ПК-12)

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 скрывание информации и ее носителей.
25. Комплексное применение методов защиты.
26. Звукоизоляция и звукопоглощение.
27. Энергетическое скрывание 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 защиты 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.

5.3.Формы и содержание рубежного контроля

Рубежный и промежуточный контроль освоения студентом дисциплины осуществляется в рамках балльно-рейтинговой системы. Распределение баллов в соответствии с действующим Положением о балльно-рейтинговой системе оценки успеваемости студентов КБГУ приведено в таблице 7.

Таблица 7

Распределение баллов в соответствии с действующим Положением о балльно-рейтинговой системе

| № рейтинговой точки | Коллоквиум | Лаб.практикум | Посещаемость | Тестирование | Итого |
|---------------------|------------|---------------|--------------|--------------|-------|
| 1 | 7 | 8 | 3 | 5 | 23 |
| 2 | 7 | 8 | 3 | 5 | 23 |
| 3 | 7 | 8 | 4 | 5 | 24 |

Таблица 8

Критерии оценки

| Вид мероприятия | Критерии оценки | Баллы |
|--|--|--------------|
| Коллоквиум (устный опрос по теме) | - ясность, четкость и доказательность изложения ответов на вопросы; - владение специальными терминами; - системность знаний по тематике | 0-21 балл |
| Лабораторное занятие | - понимание цели и задач работы - выполнение заданий и обработка результатов - отчет и защита лабораторной работы | 0-24 балла |
| Компьютерное тестирование по разделам дисциплины | Результаты тестирования (Количество баллов = $5 \cdot \varphi$, φ - доля правильно отвеченных тестов по теме). | 0-15 баллов |
| Посещение занятий | При более 3 пропусках без уважительной причины занятий аннулируются баллы | 0-10 баллов |
| Зачет | ясность, четкость и доказательность изложения ответов на вопросы; - владение специальными терминами; - системность знаний по тематике дисциплины в целом | 0-30 баллов |
| Итоговая оценка | | 0-100 баллов |

Критерии формирования оценок по промежуточной аттестации

«зачтено» – получают обучающиеся, которые относительно полно ориентируются в материале, отвечают без затруднений, допускают незначительное количество ошибок. Обучающийся способен к выполнению сложных заданий. Работа выполнена полностью, но имеются не более одной негрубой ошибки и одного недочета, не более трех недочетов. Допускаются незначительные неточности при решении задач, решено 70% задач;

«не зачтено» – получают обучающиеся, которые допускают значительные ошибки. Обучающийся имеет лишь начальную степень ориентации в материале. В работе число ошибок и недочетов превысило норму для оценки 3 или правильно выполнено менее 2/3 всей работы. Обучающийся дает неверную оценку ситуации, решено менее 50% задач.

Методические рекомендации для подготовки к зачету

Зачет является формой итогового контроля знаний и умений студентов по данной дисциплине, полученных на лекциях, лабораторных занятиях и в процессе самостоятельной работы. К зачету допускаются студенты, набравшие не менее 36 баллов по итогам текущего и промежуточного контроля. Студенты, набравшие более 61 балла по итогам промежуточного и текущего контроля, имеют право на получение зачета автоматом. На зачете студент может набрать от 15 до 30 баллов.

В период подготовки к зачету студенты вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

Подготовка студента к зачету включает три этапа:

- самостоятельная работа в течение семестра;
- непосредственная подготовка в дни, предшествующие зачету по темам курса;

- подготовка к ответу на зачетные вопросы.

При подготовке к зачету студентам целесообразно использовать материалы лекций, учебно-методические комплексы, нормативные документы, основную и дополнительную литературу.

На зачет выносится материал в объеме, предусмотренном рабочей программой учебной дисциплины за семестр. Зачет проводится в устной форме.

При проведении зачета в письменной (устной) форме, ведущий преподаватель составляет зачетные билеты, которые включают в себя: тестовые задания; теоретические задания; задачи или ситуации. Формулировка теоретических задания совпадает с формулировкой перечня зачетных вопросов, доведенного до сведения студентов накануне зачетной сессии. Содержание вопросов одного билета относится к различным разделам программы с тем, чтобы более полно охватить материал учебной дисциплины.

В аудитории, где проводится устный зачет, должно одновременно находиться не более шести студентов на одного преподавателя, принимающего зачет. На подготовку ответа на билет на зачете отводится 20 минут.

При проведении письменного зачета на работу отводится 60 минут.

Результат устного зачета выражается оценками «зачтено» и «не зачтено», дифференцированного устного зачета – оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «зачтено» выставляется, если студент показал при ответе на зачетные вопросы знание основных положений учебной дисциплины, допустил отдельные погрешности и сумел устранить их с помощью преподавателя; знаком с основной литературой, рекомендованной рабочей программой.

Оценка «не зачтено» выставляется, если при ответе на зачетные вопросы выявились существенные пробелы в знании основных положений учебной дисциплины, неумение студента даже с помощью преподавателя сформулировать правильные ответы на вопросы билета.

Контроль курсовых работ

Курсовые работы не предусмотрены.

6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ

Общий балл текущего и рубежного контроля складывается из следующих составляющих (приложение 2). Критерием оценки уровня сформированности компетенций в рамках учебной дисциплин в 5 семестре является зачет. Целью промежуточных аттестаций по дисциплине является оценка качества освоения дисциплины обучающимися.

Таблица 6. Результаты освоения учебной дисциплины, подлежащие проверке.

| Результаты обучения (компетенции) | Основные показатели оценки результатов обучения | Вид оценочного материала |
|---|---|---|
| способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и | <u>Знать</u> : цели, задачи, принципы и основные направления обеспечения информационной безопасности предприятия, угрозы предприятия на основе анализа структуры и содержания информационных процессов его, угрозы информационной | Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5) |

| | | |
|---|--|---|
| возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7) | 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 | |
| | <u>Уметь:</u> 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. | Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5) |
| | <u>Владеть:</u> 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 | Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5) |
| способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1) | <u>Знать:</u> правовые аспекты использования 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 | Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5) |

| | | |
|--|--|---|
| | информации. | |
| | <p><u>Уметь:</u> 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</p> <p>- «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.</p> | Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5) |
| | <p><u>Владеть:</u> 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</p> | Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5) |

| | | |
|---|--|--|
| | <p>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.</p> | |
| <p>способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)</p> | <p><u>Знать:</u> методы обработки экспериментальных данных при исследовании систем защиты информации, основные принципы, методы и средства измерений, используемые 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.</p> | <p>Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5)</p> |
| | <p><u>Уметь:</u> 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.</p> | <p>Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5)</p> |

| | | |
|--|---|---|
| | <u>Владеть:</u> 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. | Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5) |
|--|---|---|

7. Учебно-методическое обеспечение дисциплины

7.1. Нормативно-правовая база

1. Закон Российской Федерации от 05.03.1992 № 2446-1 "О безопасности".
2. Закон Российской Федерации от 22.06.1993 № 5485-1 "О государственной тайне".
3. Федеральный закон №128 от 08.08.2001 "О лицензировании отдельных видов деятельности"
4. Федеральный Закон №184 от 27.12.2002 "О техническом регулировании"
5. Федеральный Закон №149 от 27.07.2006 "Об информации, информационных технологиях и о защите информации"
6. Федеральный закон №152 от 27.07.2006 "О персональных данных"

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 с.— 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 с.— 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 с.— 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 с.— 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 с.— 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 с.— 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 с.— Режим доступа: <http://www.iprbookshop.ru/7000.html>.— ЭБС «IPRbooks»

7.4. Периодические издания (газета, вестник, бюллетень, журнал)

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. Современные профессиональные базы данных

1. База данных Science Index (РИНЦ) <http://elibrary.ru>
2. Национальная электронная библиотека РГБ <https://нэб.рф>
3. Крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. www.scopus.com

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

Методические рекомендации по изучению дисциплины для обучающихся

Приступая к изучению дисциплины, обучающемуся необходимо ознакомиться с тематическим планом занятий, списком рекомендованной учебной литературы. Следует уяснить последовательность выполнения индивидуальных учебных заданий, занести в свою рабочую тетрадь темы и сроки проведения семинаров, написания учебных и творческих работ. При изучении дисциплины обучающиеся выполняют следующие задания: изучают рекомендованную учебную и научную литературу; пишут контрольные работы, готовят доклады и сообщения к практическим занятиям; выполняют самостоятельные творческие работы, участвуют в выполнении практических заданий. Уровень и глубина усвоения дисциплины зависят от активной и систематической работы на лекциях, изучения рекомендованной литературы, выполнения контрольных письменных заданий

Курс изучается на лекциях, лабораторных занятиях, при самостоятельной и индивидуальной работе обучающихся. Обучающийся для полного освоения материала

должен не пропускать занятия и активно участвовать в учебном процессе. Лекции включают все темы и основные вопросы теории и практики. Для максимальной эффективности изучения необходимо постоянно вести конспект лекций, знать рекомендуемую преподавателем литературу, позволяющую дополнить знания и лучше подготовиться к лабораторным занятиям.

В соответствии с учебным планом на каждую тему выделено необходимое количество часов практических занятий, которые проводятся в соответствии с вопросами, рекомендованными к изучению по определенным темам. Обучающиеся должны регулярно готовиться к лабораторным занятиям и участвовать в обсуждении вопросов. При подготовке к занятиям следует руководствоваться конспектом лекций и рекомендованной литературой. Тематический план дисциплины, учебно-методические материалы, а также список рекомендованной литературы приведены в рабочей программе

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 обучающемуся необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.

Методические рекомендации по подготовке к лабораторным занятиям

Лабораторные занятия – составная часть учебного процесса, групповая форма занятий при активном участии обучающихся. Лабораторные занятия способствуют углубленному изучению наиболее сложных проблем науки и служат основной формой подведения итогов самостоятельной работы обучающихся. Целью лабораторных занятий является углубление и закрепление теоретических знаний, полученных обучающимися на лекциях и в процессе самостоятельного изучения учебного материала, а, следовательно, формирование у них определенных умений и навыков.

В ходе подготовки к лабораторному занятию необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой, выполнить выданные преподавателем задания. При этом учесть рекомендации преподавателя и требования программы. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы.

Желательно при подготовке к лабораторным занятиям по дисциплине одновременно использовать несколько источников, раскрывающих заданные вопросы.

Методические рекомендации по организации самостоятельной работы

Самостоятельная работа обучающихся – способ активного, целенаправленного приобретения обучающимися 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 обучающихся в подборе материала, поиске путей решения задач.

Самостоятельная работа приводит обучающихся 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:

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

Обучающимся 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 обучающийся получает в аудитории.

Необходимо отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику. При освоении курса обучающийся 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 обучающихся предусмотрена учебным планом и выполняется в обязательном порядке. Задания предложены по каждой изучаемой теме и могут готовиться индивидуально или в группе. По необходимости обучающийся может обращаться за консультацией к преподавателю. Выполнение заданий контролируется и оценивается преподавателем.

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 обучающихся и позволяет кардинальным образом изменить методику преподавания.

Обучающийся может получать все задания и методические указания через сервер, что дает ему возможность привести в соответствие личные возможности с необходимыми для выполнения работ трудозатратами. Обучающийся имеет возможность выполнять работу

дома или в аудитории. Большое воспитательное и образовательное значение в самостоятельном учебном труде обучающийся имеет самоконтроль. Самоконтроль возбуждает и поддерживает внимание и интерес, повышает активность памяти и мышления, позволяет обучающемуся 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 обучающимся 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 обучающийся 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: 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.

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.

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 зачету 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.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Требования к материально-техническому обеспечению

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.

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

8.2. 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 невидимого 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, объекты 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.

Лист переутверждения рабочей программы дисциплины

Рабочая программа:

одобрена на 2017/2018 учебный год. Протокол № __ заседания кафедры

от «__» __ 2017 г.

В рабочую программу внесены следующие изменения:

1. В части раздела «Учебно-методическое и информационное обеспечение дисциплины»

Разработчик программы _____

Зав. кафедрой _____

Одобрена на 2018-2019 учебный год.

Протокол № __ заседания кафедры от «__» __ 2018 г.

В рабочую программу внесены следующие изменения:

1. В части раздела «Учебно-методическое и информационное обеспечение дисциплины»
2. В части УП в связи с утверждением порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования, программам бакалавриата, программам специалитета, программам магистратуры (Приказ Минобрнауки №31 от 05.04.2017 г.)

Разработчик программы _____

Зав. кафедрой _____

Одобрена на 2019/2020 учебный год.

Протокол №__ заседания кафедры от «__» _____ 20__ г.

В рабочую программу внесены следующие изменения:

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 | до 30 баллов | до 10 б. | до 10 б. | до 10 б. |
| 4. | Итого сумма текущего и рубежного контроля | до 70баллов | до 23б. | до 23б | до 24б |