

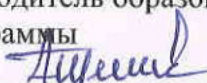
**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО
ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

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

**Институт информатики, электроники и робототехники
Кафедра электроники и цифровых информационных технологий**

СОГЛАСОВАНО

Руководитель образовательной
программы

 Р.Ш. Тешев

« 30 » 05 2023 г.

УТВЕРЖДАЮ

И.о. директора ИИЭиР



 Р.Ш. Тешев

« 30 » 05 2023 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Б1.В.ДВ.01.02.ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ
ЗАЩИТЫ ИНФОРМАЦИИ**

Направление подготовки
11.04.01 Радиотехника

Магистерская программа
**Интегрированные системы безопасности с
распределенной архитектурой**

Квалификация (степень) выпускника
Магистр

Форма обучения
Очная

Нальчик 2023

Рабочая программа дисциплины (модуля) «Технические средства и методы защиты информации» /составители О.Г.Ашхотов, И.Б. Ашхотова, Нальчик, КБГУ, 2023. 22 с.

Рабочая программа дисциплины (модуля) «Технические средства и методы защиты информации» вариативной части дисциплин по выбору – Б1.В.ДВ.01.02 предназначена для магистров очной формы обучения по направлению подготовки 11.04.01 Радиотехника профиль Интегрированные системы безопасности с распределенной архитектурой, обучающимся в 1 семестре, 1 курса.

Рабочая программа дисциплины (модуля) «Технические средства и методы защиты информации» составлена с учетом федерального государственного образовательного стандарта высшего образования по направлению подготовки 11.04. 01 Радиотехника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 года № 925.

Содержание

1. Цель и задачи освоения дисциплины (модуля).....	4
2. Место дисциплины (модуля) в структуре ОПОП ВО.....	4
3. Требования к результатам освоения дисциплины(модуля)	4
4. Содержание и структура дисциплины (модуля).....	5
Структура дисциплины (модуля)	7
5. Оценочные материалы для текущего и рубежного контроля успеваемости и промежуточной аттестации.....	8
5.1. Коллоквиум	8
5.2. Образцы тестовых заданий	8
Методические рекомендации по подготовке к тестированию.....	9
Критерии оценивания.....	10
5.3. Задания для лабораторных занятий	11
6. Промежуточная аттестация.....	11
7. Контроль курсовых работ.....	13
8. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности.....	15
9. Учебно-методическое обеспечение дисциплины (модуля).....	16
Основная литература	16
Дополнительная литература	16
Периодические издания.....	16
Интернет-ресурсы.....	16
10. Программное обеспечение современных информационно-коммуникационных технологий.....	17
11. Материально-техническое обеспечение дисциплины.....	20
Лист изменений (дополнений) в рабочей программе дисциплины (модуля)	22

1. Цели и задачи освоения дисциплины

Цель курса: изучение технических средств и методов защиты информации автоматизированных систем обработки информации и управления; ремонт и техническое обслуживание этой аппаратуры. Тенденции и перспективы развития дисциплины «Технические средства и методы защиты информации» определяются центральной проблемой информационных систем – проблемой обеспечения безопасности работы и эксплуатации.

Основными задачами изучения дисциплины являются следующие представления о:

- видах, источниках и носителях защищаемой информации;
- классификации технической разведки;
- методах и средствах инженерной защиты и технической охраны объектов;
- возможностях видов технической разведки;
- характеристик государственной системы противодействия технической разведке;
- основных положений методологии инженерно-технической защиты информации.

Изучение дисциплины направлено на подготовку специалистов, способных решать проблемы, возникающие при эксплуатации изделий электронной техники с учетом области, типов и задач профессиональной деятельности в соответствии с профессиональными стандартами:

- 06.005 «Специалист по эксплуатации радиоэлектронных средств (инженер-электроник)», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 31 июля 2019 года N 540н (зарегистрирован в Минюсте РФ 28 августа 2019 года, регистрационный N55756).
- 40.058 «Инженер-технолог по производству изделий микроэлектроники», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 03.07.2019 г. № 480н (зарегистрирован Минюстом России 29.07.2019 г. №55439).

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Технические средства и методы защиты информации» в структуре ОПОП ВО включена в вариативную часть дисциплин по выбору блока Б1.В.ДВ.01.02 и изучается магистрами 11.04.01 Радиотехника, профиль Интегрированные системы безопасности с распределенной архитектурой в 1 семестре 1 курса.

При освоении дисциплины обучающийся сможет частично продемонстрировать следующие обобщенные трудовые функции (ОТФ):

- **Эксплуатация радиоэлектронной аппаратуры** (профессиональный стандарт 06.005 «Специалист по эксплуатации радиоэлектронных средств (инженер-электроник)», код В, уровень квалификации -5);
- **Разработка единичных технологических процессов и рекомендаций по устранению и предупреждению брака в производстве изделий микроэлектроники** (профессиональный стандарт 40.058 «Инженер-технолог по производству изделий микроэлектроники», код В, уровень квалификации -6).

Дисциплина опирается на знания, умения и компетенции, приобретенные и сформированные в результате изучения дисциплин: «Методы и средства защиты объектов», «Компьютерные технологии в научных исследованиях», «Системы контроля управления доступом».

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:

- **профессиональных компетенций (ПК):**
 - Способен проводить ввод в эксплуатацию, техническое обслуживание и текущий ремонт радиоэлектронных комплексов (ПКС-М.1);
 - Способен к разработке и адаптации типовых технологических процессов изготовления изделий микроэлектроники (ПКС-М.2).

(профессиональный стандарт 06.005 «Специалист по эксплуатации радиоэлектронных средств

(инженер-электроник)», трудовая функция В/01.5 - Техническое обслуживание радиоэлектронной аппаратуры).

В результате изучения дисциплины (модуля) студент должен:

Знать:

- методы технического обеспечения эксплуатации радиоэлектронных комплексов;
- принципы работы, устройство, технические возможности средств контроля технического состояния радиоэлектронных комплексов и перспективы их совершенствования;

Уметь:

- использовать оборудование для диагностирования и устранения неисправностей, возникших при эксплуатации радиоэлектронных комплексов;
- производить замену ответственных узлов и элементов радиоэлектронных комплексов.

Владеть:

- изучением руководства по эксплуатации радиоэлектронных комплексов, содержащего сведения о конструкции, принципе действия, характеристиках радиоэлектронных комплексов и их составных частей;
- изучением инструкций по монтажу, настройке, пуску и обкатке радиоэлектронных комплексов и их составных частей;
- тестированием работы радиоэлектронных комплексов при вводе их в эксплуатацию;

4. **Содержание и структура дисциплины** *Содержание разделов дисциплины*

Таблица 1

№ Раздела	Наименование раздела	Содержание раздела	Код контролируемой компетенции (или ее части)	Форма текущего контроля
1	Введение	Структура курса. Рейтинговые мероприятия. Рекомендуемая литература. Цель и задачи курса. Терминология, некоторые определения и понятия.	ПКС-М.1 ПКС-М.2	ЛР, К, РК, Т
2	Основные понятия информационной безопасности	Глобализация инфосферы и связанные с этим угрозы обществу. Основные понятия информационной безопасности. Угрозы и цели защиты информации. Формы представления информации. Основные направления защиты.	ПКС-М.1 ПКС-М.2	ЛР, К, РК, Т
3	Методы и средства защиты объектов информатизации	Организация защиты информации в РФ. Понятия о видах разведки. Мероприятия по противодействию техническим разведкам. Основные методы добывания информации. Физические принципы образования каналов утечки и способов защиты информации. Методы и средства защиты информации от утечки из помещений, от технических средств по эфиру и линиям связи.	ПКС-М.1 ПКС-М.2	ЛР, К, РК, Т

4	Комплексный подход к обеспечению информационной безопасности	Основные положения концепции инженерно-технической защиты информации. Характеристика защищаемой информации. Виды, источники и носители защищаемой информации; демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники. Основные понятия информационной безопасности. Угрозы безопасности информации и каналы утечки информации. Инженерно-техническая, криптографическая и программно-аппаратная защита информации.	ПКС-М.1 ПКС-М.2	ЛР, К, РК, Т
5	Защита от несанкционированного доступа к информации в компьютерных системах	Способы несанкционированного доступа к информации и защиты от него. Способы аутентификации пользователей компьютерных систем. Протоколы аутентификации при удаленном доступе. Методы управления доступом к объектам компьютерных систем. Средства защиты информации в глобальных вычислительных сетях. Стандарты безопасности компьютерных систем и информационных технологий. Способы симметрического шифрования. Абсолютно стойкий шифр. Принципы создания и свойства асимметрических криптосистем. Электронная цифровая подпись. Функции хеширования. Компьютерная стеганография.	ПКС-М.1 ПКС-М.2	ЛР, К, РК, Т
6	Характеристика угроз безопасности информации	Побочные электромагнитные излучения и наводки. Технические каналы утечки информации. Методы добывания информации. Методы инженерно-технической защиты информации.	ПКС-М.1 ПКС-М.2	ЛР, К, РК, Т
7	Методы физической защиты информации	Методы противодействия наблюдению. Методы противодействия подслушиванию. Экранирование побочных излучений и наводок.	ПКС-М.1 ПКС-М.2	ЛР, К, РК, Т
8	Защита от вредоносных программ	Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и защита от них.	ПКС-М.1 ПКС-М.2	ЛР, К, РК, Т
9	Защита от несанкционированного копирования информации информационных ресурсов	Принципы построения и состав систем защиты от несанкционированного копирования. Методы защиты от копирования инсталляционных дисков и установленного программного обеспечения.	ПКС-М.1 ПКС-М.2	ЛР, К, РК, Т

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

Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов)

Таблица 2.

Вид работы	Трудоемкость, часы	
	1 семестр	Всего
Общая трудоемкость (в часах)	108	108
Контактная работа (в часах):	34	34
<i>Лекционные занятия (Л)</i>	17	17
<i>Лабораторные работы (ЛР)</i>	17	17
Самостоятельная работа (в часах), в том числе контактная работа:	65	65
Курсовая работа (КР)/ Курсовой проект (КП)	3	3
Самостоятельное изучение разделов/тем	62	62
Подготовка и прохождение промежуточной аттестации	9	9
Вид промежуточной аттестации	Зачет, курсовая работа	

Лекционные занятия

Таблица 3

№	Тема
1	Введение
2	Основные понятия информационной безопасности
3	Методы и средства защиты объектов информатизации
4	Комплексный подход к обеспечению информационной безопасности
5	Защита от несанкционированного доступа к информации в компьютерных системах
6	Характеристика угроз безопасности информации
7	Методы физической защиты информации
8	Защита от вредоносных программ
9	Защита от несанкционированного копирования информационных ресурсов

Лабораторные работы

Таблица 4.

№	Тема
1	Маскировка. Техническая реализация маскировки средств вычислительной техники. Использование ЛГШ, Гром 3И-4Б
2	Обнаружение радиозакладок. Статистический анализ загрузки заданного диапазона и обнаружение закладок в помещении при помощи Пиранья-Р.
3	Сетевые закладки. Обнаружение сигналов линейных и сетевых закладок при помощи Пиранья-Р.
4	ИК-диапазон. Анализ ИК диапазона при помощи Пиранья-Р
5	Анализ поля. Обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля при помощи индикатора Комар, использование подавителя радиопередатчиков Вето-М.
6	ПЭМИН по электрической составляющей. Обнаружение ПЭМИН по электрической составляющей электромагнитного поля с помощью спрут-мини

7	ПЭМИН по магнитной составляющей. Обнаружение ПЭМИН по магнитной составляющей электромагнитного поля с помощью спрут-мини
8	Измерение наводок в цепях электропитания. Обнаружение ПЭМИН в электрических цепях с помощью пробника напряжения П1
9	Акустический канал. Оценка защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу комплексом R&S® FS300, с использованием шумомеров и измерителей уровня вибрации ВШВ-003-МЗ, Robotron 00023

Самостоятельное изучение разделов дисциплины

Таблица 5.

№	Вопросы, выносимые на самостоятельное изучение
1	Основные методы добывания информации. Ознакомление с техническими возможностями некоторых средств перехвата информации из помещений, от технических средств по эфиру и линиям связи.
2	Физические принципы образования каналов утечки и способов защиты информации. Методы и средства защиты информации от утечки из помещений, от технических средств по эфиру и линиям связи.
3	Общие понятия о возможных методах несанкционированного, в том числе деструктивного, воздействия на информационные ресурсы и оборудование информационных систем. Электромагнитный и кибер терроризм.
4	Теоретические основы инженерно-технической защиты информации. Характеристика защищаемой информации. Виды, источники и носители защищаемой информации; демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники.
5	Способы несанкционированного доступа к информации и защиты от него. Способы аутентификации пользователей компьютерных систем. Протоколы аутентификации при удаленном доступе. Методы управления доступом к объектам компьютерных систем.
6	Средства защиты информации в глобальных вычислительных сетях. Разграничение полномочий и управление доступом к ресурсам в защищенных версиях ОС Windows. Разграничение полномочий и управление доступом к ресурсам в ОС Unix.
7	Стандарты безопасности компьютерных систем и информационных технологий. Способы симметрического шифрования. Современные алгоритмы симметрического шифрования. Абсолютно стойкий шифр. Принципы создания и свойства асимметрических криптосистем. Примеры асимметрических криптосистем.
8	Электронная цифровая подпись и ее использование. Функции хеширования. Принципы использования криптографического интерфейса ОС Windows. Компьютерная стеганография и ее применение.
9	Побочные электромагнитные излучения и наводки. Технические каналы утечки информации. Методы добывания информации. Методы инженерно-технической защиты информации
10	Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и защита от них.
11	Методы противодействия наблюдению. Методы противодействия подслушиванию. Экранирование побочных излучений и наводок

5. Оценочные материалы для текущего и рубежного контроля успеваемости и промежуточной аттестации

5.1.

Коллоквиум

В семестре проводятся 3 коллоквиума, которые оцениваются по 8 баллов каждый.

Вопросы, выносимые на коллоквиум
(контролируемые компетенции ПК-1)

Первый коллоквиум

1. Основные понятия информационной безопасности. Угрозы и цели защиты информации.
2. Формы представления информации. Основные направления защиты.
3. Организация защиты информации в РФ. Понятия о видах разведки.
4. Мероприятия по противодействию техническим разведкам. Основные методы добычи информации.
5. Технические возможности некоторых средств перехвата информации из помещений, технические средства по эфиру и линиям связи.
6. Физические принципы образования каналов утечки и способов защиты информации. Методы и средства защиты информации от утечки из помещений, от технических средств по эфиру и линиям связи
7. Основные положения концепции инженерно-технической защиты информации.
8. Теоретические основы инженерно-технической защиты информации.
9. Угрозы безопасности информации и каналы утечки информации. Комплексный подход к защите информации.

Второй коллоквиум

1. Организационная защита информации.
2. Правовое обеспечение информационной безопасности.
3. Инженерно-техническая, криптографическая и программно-аппаратная защита информации.
4. Способы несанкционированного доступа к информации и защиты от него.
5. Способы аутентификации пользователей компьютерных систем.
6. Методы управления доступом к объектам компьютерных систем.
7. Средства защиты информации в глобальных вычислительных сетях
8. Стандарты безопасности компьютерных систем и информационных технологий.
9. Способы симметрического шифрования. Современные алгоритмы симметрического шифрования.

Третий коллоквиум

1. Принципы создания и свойства асимметрических криптосистем.
2. Электронная цифровая подпись и ее использование. Функции хеширования.
3. Принципы использования криптографического интерфейса ОС Windows. Компьютерная стеганография и ее применение.
4. Побочные электромагнитные излучения и наводки.
5. Технические каналы утечки информации. Методы добывания информации. Методы инженерно-технической защиты информации.
6. Методы противодействия наблюдению. Методы противодействия подслушиванию.
7. Экранирование побочных излучений и наводок. Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и защита от них.
8. Принципы построения и состав систем защиты от несанкционированного копирования.
9. Методы защиты от копирования установочных дисков и установленного программного обеспечения.

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 2 балла	удовлетворительно 4 балла	хорошо 6 баллов	отлично 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.

5.2.

Образцы тестовых заданий

(контролируемые компетенции ПК-1)

№ 1. Различают следующие категории объектов защиты

- а) по степени важности
- б) по размеру нанесенного ущерба объекту, окружающей среде, общественным структурам
- в) нанесение вреда здоровью и жизни людей, экологии и т.д.
- г) по коммерческому ущербу

№ 2. Особенности задач охраны различных типов объектов (два верных ответа)

- +: На ОВ объектах необходимо нейтрализовать злоумышленника до того, как он выполнит намеченные действия.
- +: На ПК объектах нарушителя нейтрализовать как до, так и после совершения акции.
- : Реализовать только видеонаблюдение на объектах
- : На ОВ объектах нет необходимости нейтрализовывать злоумышленника
- : Реализовать только видеонаблюдение на объектах

№ 3. Основные задачи, решаемые физическими средствами защиты (верны 4 ответа):

- +: Охрана территории, оборудования, внутренних помещений и наблюдение за ними.
- : Уборка территории предприятия.
- +: Осуществление контролируемого доступа в контролируемые зоны.
- +: Противопожарная защита.
- +: Блокирование действий злоумышленника.
- : Оповещение всего населения об опасности.

№ 4. Адекватные меры защиты предусматривают:

- а) тотальный контроль несанкционированного проникновения на территорию объекта, в здания и помещения;
- б) ограничение и контроль доступа людей в «закрытые» здания и помещения с возможностью документирования результатов контроля;
- в) обнаружение злоумышленника на самых ранних этапах его продвижения к цели акции;
- г) оценку ситуации;

№ 5. Система обеспечения безопасности включает в себя (4 верных ответа)

- + Система охранно-тревожной сигнализации
- Система медицинского мониторинга служащих.
- + Система контроля и управления доступом
- + Система пожарной сигнализации
- + Система периметровой охраны
- Система оповещения населения об опасности.

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 выяснить 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.

5.3.

Задания для лабораторных занятий (контролируемые компетенции ПК-1)

Лабораторный практикум является важным элементом обучения, т.к. прививает навыки самостоятельной работы на различном лабораторном оборудовании и умение пользоваться различными приборами и инструментами.

Пример типовой лабораторной работы «Конфигурирование цифровой системы видеонаблюдения»

Цель работы: получение практических навыков конфигурирования цифровой системы видеонаблюдения.

Методические указания

Выполнение каждой лабораторной работы складывается из следующих этапов.

1. Самостоятельная подготовка студентов к работе. Перед началом работы студенты должны четко представлять себе цель работы, сущность ожидаемых результатов. Студенты, неподготовившиеся к работе в соответствии с этими требованиями, к выполнению работы не допускаются.

2. Проведение эксперимента. Этот этап осуществляется в соответствии с методическими указаниями, которые содержатся в описании к каждой работе. Лабораторные измерения на стенде студент может начать только после собеседования с преподавателем и получения соответствующего допуска. Результаты работы проверяются преподавателем.

При работе в лаборатории необходимо строго выполнять все правила техники безопасности и указания преподавателя.

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:

- задание;
- описание работы;
- полученные результаты за подписью преподавателя;
- общие выводы о работе и заключение, о качестве выполненной работы.

Текст отчета должен быть написан аккуратно и разборчиво от руки или представлен в виде распечатки, после компьютерной верстки. В обоих случаях текст должен представлять собой логическое изложение существа вопроса. Отчет должен быть понятен для каждого читающего без каких-либо дополнительных вопросов у составителей отчета.

4. После представления отчета студент должен иметь, как минимум, поверхностные знания по контрольным вопросам к работе, имеющимся в методических указаниях, и ему выставляется балл, которым оценена данная лабораторная работа.

6. Промежуточная аттестация (контролируемые компетенции ПК-1)

Список основных вопросов к устному зачету

1. Глобализация инфосферы и связанные с этим угрозы обществу. Основные понятия информационной безопасности.
2. Угрозы и цели защиты информации. Формы представления информации. Основные направления защиты.
3. Организация защиты информации в РФ. Понятия о видах разведки. Мероприятия по противодействию техническим разведкам.
4. Основные методы добывания информации.
5. Технические возможности некоторых средств перехвата информации из помещений, технических средств по эфиру и линиям связи.
6. Физические принципы образования каналов утечки и способов защиты информации.
7. Методы и средства защиты информации от утечки из помещений, от технических средств по эфиру и линиям связи.
8. Основные положения концепции инженерно-технической защиты информации. Теоретические основы инженерно-технической защиты информации.
9. Угрозы безопасности информации и каналы утечки информации. Комплексный подход к защите информации. Организационная защита информации.
10. Правовое обеспечение информационной безопасности. Инженерно-техническая, криптографическая и программно-аппаратная защита информации.
11. Способы несанкционированного доступа к информации и защиты от него. Способы аутентификации пользователей компьютерных систем.

12. Методы управления доступом к объектам компьютерных систем. Средства защиты информации в глобальных вычислительных сетях.
13. Стандарты безопасности компьютерных систем и информационных технологий. Способы симметрического шифрования. Современные алгоритмы симметрического шифрования.
14. Принципы создания и свойства асимметрических криптосистем. Электронная цифровая подпись и ее использование. Функции хеширования.
15. Принципы использования криптографического интерфейса ОС Windows. Компьютерная стеганография и ее применение.
16. Побочные электромагнитные излучения и наводки. Технические каналы утечки информации. Методы добывания информации. Методы инженерно-технической защиты информации.
17. Методы противодействия наблюдению. Методы противодействия подслушиванию. Экранирование побочных излучений и наводок.
18. Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и защита от них.
19. Принципы построения и состав систем защиты от несанкционированного копирования. Методы защиты от копирования инсталляционных дисков и установленного программного обеспечения.
20. Инженерные средства защиты. Технические средства охраны, в том числе электронные средства: средства обнаружения, средства коммуникации.

Методические рекомендации при подготовке к зачету

Подготовка студентов к зачету включает проработку лекций, в течение семестра и непосредственную подготовку в дни, предшествующие зачету, включая, конечно, подготовку к коллоквиумам, тестированию, выполнению лабораторных работ и их защите.

Для подготовки к ответам вопросы зачета (они выдаются в конце семестра) студент должен использовать не только курсы лекций, но и основную и дополнительную литературу для выработки умения давать развернутые ответы на поставленные вопросы.

В ходе подготовки к зачету студенту необходимо обращать внимание не только на уро-вень запоминания, но и на степень понимания изучаемых вопросов. Это достигается не про-стым заучиванием, а усвоением прочных систематизированных знаний аналитическим мыш-лением. Следовательно, непосредственная подготовка к зачету должна в разумных propor-циях сочетать и запоминание, и понимание программного материала.

Распределение баллов текущего, рубежного контроля

№		Общая сумма	1-я точка	2-я точка	3 точка
1.	Текущий контроль				
	посещение занятий	10 баллов	3 балла	3 балла	4 балла
	выполнение и защита лабораторных работ	21 балл	7 баллов	7 баллов	7 баллов
2.	Рубежный контроль				
	Тестирование	15 баллов	5 баллов	5 баллов	5 баллов
	Коллоквиум	24 балла	8 баллов	8 баллов	8 баллов
Итого		70 баллов	23 балла	23 балла	24 балла

Критерии оценивания

При освоении дисциплины формируются компетенции ПК-1. Указанные компетенции формируются в соответствии со следующими этапами:

- формирование и развитие теоретических знаний, предусмотренных указанными компетенциями (лекционные занятия, самостоятельная работа студентов);
- приобретение и развитие практических умений, предусмотренных компетенциями (лабораторные работы, самостоятельная работа студентов);
- закрепление теоретических знаний, умений и практических навыков, предусмотренных компетенциями (лабораторные работы, практики, выпускная квалификационная работа).

Критерии оценки качества освоения дисциплины, завершающейся зачетом

<i>Баллы (рейтин- говой оценки)</i>	<i>Результат освоения</i>	<i>Требования уровню сформированности компетенций</i>
61-70	Зачтено (без проце- дуры сдачи за- чета)	Обучающийся освоил знания, умения и навыки, входящие в состав компетенций: ПК-1 Способен проводить ввод в эксплуатацию, техническое обслуживание и текущий ремонт радиоэлектронных комплексов
36-61	Зачтено (с процедурой сдачи зачета)	Обучающийся проявляет компетенции ПК-1, но не в полном объеме входящих в их состав действий. Обучающийся может допустить некоторые неточности, негрубые ошибки, затрудняться в изложении материала, но правильно отвечать на задаваемые ему вопросы.
менее 36 балла	не допущен к зачету	Компетенции не сформированы

«Зачтено» выставляется обучающемуся, продемонстрировавшему полное, всестороннее, осознанное правильное знание программного материала и изложившему ответ логично, грамотно, убедительно, готового к дальнейшему профессиональному совершенствованию.

При ответе обучающийся может допустить некоторые неточности, негрубые ошибки, затрудняться в самостоятельном изложении материала, но правильно отвечать на задаваемые ему вопросы, в результате наводящих вопросов с помощью преподавателя исправлять допущенные ошибки и неточности.

«Незачтено» может быть выставлено обучающемуся, обнаружившему неполное, неосознанное знание учебно-программного материала, допускающему грубые ошибки, неспособному самостоятельно изложить ответ на вопрос, отвечающему неправильно или не дающему ответ на заданные вопросы. Демонстрируемый уровень знаний не может быть признан достаточным для профессиональной деятельности.

7. Курсовой проект (курсовая работа)

(контролируемые компетенции ПК-1)

1. Системный подход к защите информации. Основные концептуальные положения инженерно-технической защиты информации.
2. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации.
3. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Показатели эффективности инженерно-технической защиты информации.
4. Информация как предмет защиты. Источники опасных сигналов.

5. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие о текущей и эталонной признаковой структуре.
6. Основные и вспомогательные технические средства и системы как источники опасных сигналов.
7. Технические каналы утечки информации.
8. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика и возможности.
9. Методы добывания информации. Методы инженерной защиты и технической охраны объектов.
10. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой.
11. Классификация технической разведки. Возможности видов технической разведки. Основные направления развития технической разведки.
12. Классификация способов инженерной защиты и технической охраны объектов. Инженерные конструкции. Автономные и централизованные системы охраны. Автоматизация процессов охраны.
13. Методы скрытия информации и ее носителей.
14. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрытие радио- и электрических сигналов. Виды и условия зашумления.
15. Средства предотвращения утечки информации по техническим каналам.
16. Государственная система защиты информации. Контроль эффективности инженерно-технической защиты информации.
17. Виды контроля эффективности инженерно-технической защиты информации. Виды зон безопасности. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации.
18. Моделирование и принципы оценки эффективности инженерно-технической защиты информации.
19. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты.
20. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации.

Требования к курсовой работе

Курсовая работа (проект) - вид учебной работы по изучаемой дисциплине (модулю), предусмотренный рабочим учебным планом и выполняемый студентом самостоятельно под руководством преподавателя.

Целью курсовой работы (проекта) является закрепление и систематизация теоретических знаний в ходе самостоятельного изучения исследовательской проблемы.

Задачи курсовой работы (проекта):

- проверка знаний, полученных студентом в ходе изучения дисциплин;
- формирование умений самостоятельной работы с литературой.

Курсовая работа (проект) должна представлять собой завершённое исследование, в котором анализируются исследовательские проблемы в рассматриваемой области, и раскрывается содержание и технологии разрешения этих проблем не только в теоретическом, но и в практическом плане на местном, региональном или федеральном уровнях. Работа должна носить творческий характер, отвечать требованиям логического и чёткого изложения материала, доказательности и достоверности фактов, отражать умения студента пользоваться рациональными приёмами поиска, отбора, обработки и систематизации информации и содержать теоретические выводы и практические рекомендации.

Курсовая работа (проект) должна содержать следующие структурные элементы:

- титульный лист;
- оглавление (если текст работы делится на главы) или содержание (в том случае, если текст работы делится на разделы);
- введение;
- основная часть;
- заключение;
- библиографический список;
- графическая часть (при необходимости);
- приложения (при необходимости).

Выполнение курсовой работы складывается из нескольких этапов: анализ литературных и иных источников информации, составление плана работы, накопление и обработка фактического материала, написание и оформление работы, защита курсовой работы (проекта).

Завершённая курсовая работа (проект) за неделю до защиты представляется студентом руководителю, который решает вопрос о допуске студента к защите курсовой работы (проекта).

Результаты защиты курсовой работы (проекта) оцениваются дифференцированной отметкой («отлично», «хорошо», «удовлетворительно»), которая записывается в ведомость и зачётную книжку студента. Оценка «неудовлетворительно» проставляется в экзаменационную ведомость, в зачётную книжку не вносится.

Критерии оценивания курсовой работы

Оценка			
неудовлетворительно менее 61 балла	удовлетворительно 61-80 баллов	хорошо 81-90 баллов	отлично 91-100 баллов
Работа выполнена не в соответствии с утвержденным планом, не раскрыто содержание каждого вопроса. Студентом не сделаны выводы по теме работы. Грубые недостатки в оформлении работы. При защите работы студент не владеет материалом, не отвечает на вопросы.	Работа выполнена в соответствии с утвержденным планом, но не полностью раскрыто содержание каждого вопроса. Студентом не сделаны собственные выводы по теме работы. Грубые недостатки в оформлении работы. При защите работы студент слабо владеет материалом, отвечает не на все вопросы.	Работа выполнена в соответствии с утвержденным планом, полностью раскрыто содержание каждого вопроса. Незначительные замечания к оформлению работы. При защите работы студент владеет материалом, но отвечает не на все вопросы.	Работа выполнена в соответствии с утвержденным планом, полностью раскрыто содержание каждого вопроса, студентом сформулированы собственные аргументированные выводы по теме работы. Оформление работы соответствует предъявляемым требованиям. При защите работы студент свободно владеет материалом и отвечает на вопросы.

8. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности

Результаты освоения учебной дисциплины, подлежащие проверке.

Таблица 6.

Результаты обучения (компетенции)	Основные показатели оценки результатов обучения	Вид оценочного материала
<p>Способен проводить ввод в эксплуатацию, техническое обслуживание и текущий ремонт радиоэлектронных комплексов (ПК-1) (профессиональный стандарт 06.005 «Специалист по эксплуатации радиоэлектронных средств (инженер-электроник)», трудовая функция В/01.5 - Техническое обслуживание радиоэлектронной аппаратуры).</p> <p>Код и наименование индикатора достижения компетенции:</p> <p>ПК-1.1 Анализирует методы технического обеспечения эксплуатации радиоэлектронных комплексов.</p> <p>ПК-1.2 Проводит мониторинг и диагностику технического состояния радиоэлектронных комплексов</p>	<p>Знать:</p> <p>-методы технического обеспечения эксплуатации радиоэлектронных комплексов;</p> <p>-принципы работы, устройство, технические возможности средств контроля технического состояния радиоэлектронных комплексов и перспективы их совершенствования;</p>	<p>Выполнение и защита лабораторных работ;</p> <p> типовые оценочные материалы для устного опроса (<i>раздел 5.1.1</i>);</p> <p> типовые тестовые задания (<i>раздел 5.2</i>);</p> <p> типовые оценочные материалы (<i>раздел 6</i>).</p>
	<p>Уметь:</p> <p>-использовать оборудование для диагностирования и устранения неисправностей, возникших при эксплуатации радиоэлектронных комплексов;</p> <p>-производить замену ответственных узлов и элементов радиоэлектронных комплексов.</p>	<p>Выполнение и защита лабораторных работ;</p> <p> типовые оценочные материалы для устного опроса (<i>раздел 5.1.1</i>);</p> <p> типовые тестовые задания (<i>раздел 5.2</i>);</p> <p> типовые оценочные материалы (<i>раздел 6</i>).</p>
	<p>Владеть:</p> <p>-изучением руководства по эксплуатации радиоэлектронных комплексов, содержащего сведения о конструкции, принципе действия, характеристиках радиоэлектронных комплексов и их составных частей;</p> <p>-изучением инструкций по монтажу, настройке, пуску и обкатке радиоэлектронных комплексов и их составных частей;</p> <p>- тестированием работы радиоэлектронных комплексов при вводе их в эксплуатацию.</p>	<p>Выполнение и защита лабораторных работ;</p> <p> типовые оценочные материалы для устного опроса (<i>раздел 5.1.1</i>);</p> <p> типовые тестовые задания (<i>раздел 5.2</i>);</p> <p> типовые оценочные материалы (<i>раздел 6</i>).</p>

9. Учебно-методическое обеспечение дисциплины(модуля)

Основная литература

1. Ерохин В.В. Безопасность информационных систем. - М.: ФЛИНТА, 2015. <http://www.studentlibrary.ru/book/ISBN9785976519046.html>
2. Аверченков В.И. Методы и средства инженерно-технической защиты информации. Брянск: БГТ ун-т. 2012. <http://www.iprbookshop.ru/7000.html>
3. Горев А.И. Обработка и защита информации в компьютерных системах. —Омск: Омская академия МВД. 2016. <http://www.iprbookshop.ru/72856.html>

Дополнительная литература

1. Основы информационной безопасности: Учебник. – Воронеж, 2001.
2. Андрианов В.И., Соколов А.В. Устройства для защиты объектов и информации: Справ. пособие. - М.: АСТ. СПб.: Полигон, 2000.
3. Андрианов В.И., Бородин В.А., Соколов А.В. «Шпионские штучки» и устройства для защиты объектов и информации: Справ. пособие. – СПб.: Лань, 1996.
4. Барабанов Н.П., Кленов С.Н. Обеспечение безопасности информации в уголовно-исполнительной системе. – Рязань: Академия права и управления Минюста России, 2003.
5. Рудометов Е.А., Рудометов В.Е. Электронные средства коммерческой разведки и защиты информации: Справ. пособие. – СПб.: Полигон, М.: АСТ, 2000.
6. Организация охраны и совершенствование оборудования объектов УИС инженерно-техническими средствами охраны и надзора: Сб. материалов положит. опыта. М.: НИИ ФСИН России, 2007.

Периодические издания

Перечень периодических изданий, получаемых библиотекой КБГУ, в которых студент может ознакомиться с современными достижениями в области методов и средств защиты объектов: Журнал «Алгоритм безопасности», Технологии защиты, Безопасность, Мониторинг. Наука и безопасность.

Интернет ресурсы

1. <http://lib.kbsu.ru/>- Библиотека КБГУ.
2. <http://www.garant.ru/> - Справочная правовая система «Гарант».
3. <http://www.consultant.ru/>- Справочная правовая система «КонсультантПлюс».
4. http://www.ph4s.ru/book_electronika.html- Образовательный проект А.Н.Варгина
5. <http://www.Russianelectronics.ru>-портал «Времяэлектроники»;
6. <http://www.platan.ru>– каталог электронных компонентов;
7. <http://metodist.lbz.ru/iiumk/nano/lections.php> - видеоролики по нанотехнологии;
8. <http://nano.fcior.edu.ru>– каталог научно- образовательных ресурсов для нанотехнологии.
9. <https://www.sciencedirect.com/>- Полнотекстовая база данных ScienceDirect.
10. <https://threatpos>– новости информационной безопасности
11. | <https://www.anti-malware.ru/>- информационная безопасность для профессионалов
12. <https://geektimes.ru/hub/infosecurity/>- информационная безопасность. Защита данных.
13. <http://safe.cnews.ru/>- интернет-издание о высоких технологиях

10. Программное обеспечение современных информационно-коммуникационных технологий

1. Студенты имеют доступ к единому образовательному portalу, 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. При выполнении лабораторного практикума студенты в обязательном порядке проводят обработку экспериментальных данных с применением программных сред MS Excel, MathCad.

4. В рамках обеспечения применения компьютерных технологий в образовательном процессе имеются специализированные компьютерные классы с современным программным обеспечением и имеющим выход в Интернет.

11. Материально-техническое обеспечение дисциплины

Материально-техническую базу для проведения занятий по дисциплине составляют:

- специализированная аудитория, используемая при проведении занятий лекционного типа №238, расположенная по адресу: 360004, Кабардино-Балкарская республика, г. Нальчик, ул. Чернышевского, 175, учетный номер №14, оснащенная мультимедийным проектором и комплектом аппаратуры, позволяющей демонстрировать текстовые и графические материалы;
- рабочее место преподавателя;
- рабочие места студентов;
- меловая доска.

Мультимедийная презентация, сопровождающая лекцию, позволяет преподавателю акцентировать внимание студенческой аудитории на ключевых вопросах лекции.

Дисциплина обеспечена:

- тестовым материалом в электронной обучающей системе «Moodle» (Открытый университет);
- книжным фондом библиотеки;
- электронными версиями лекций и учебников.

Лабораторные занятия проводятся в лаборатории №129, расположенной по адресу: 360004, Кабардино-Балкарская республика, г. Нальчик, ул. Чернышевского, 175, учетный номер №14. Лаборатория оснащена необходимым программным обеспечением и оборудованием: Система контроля и управления доступом (СКУД) ВЕРСЕТ – GSM 03BM; Прибор приемно-контрольный охранно-пожарный "СИГНАЛ-20М"; Прибор приемно-контрольный охранно-пожарный КАРАТ-(М).

Студенты имеют доступ через Интернет к электронной обучающей системе «Moodle» (Открытый университет), которая позволяет размещать электронные учебные курсы в свободном доступе для студентов университета.

При проведении занятий лекционного типа и лабораторных занятий используются: **лицензионное программное обеспечение и свободно распространяемые программы:**

- Microsoft Office лицензия: Договор №135 от 22.05.2018, договор № л-21100 от 20.09.2017, сертификат от 29.11.2017, договор № 28/2017-31705322460 от 29.08.2017, договор № 18/2016-31603884322 от 12.08.2016, договор № 4/14-08 от 14.08.2015, договор № 1/01-12 от 01.12.2014, договор №0331100002314000061-0003152-01 от 25.11.2014, договор №0331100002314000077-0003152-01 от 29.12.2014, договор №0331100002314000038-0003152-01 от 10.09.2014, сертификат от 20.04.2009, сертификат от 18.06.2008, сертификат от 12.10.2007, сертификат от 14.03.2007;
- архиватор 7z, Adobe Acrobat Reader лицензия: предоставляется бесплатно на условиях по адресу <https://www.adobe.com/ru/legal/terms.html>;
- Mozilla Firefox лицензия: GPL/LGPL/MPL, Google Chrome лицензия: предоставляется бесплатно на условиях лицензионных соглашений на программное обеспечение с открытым исходным кодом по адресу <https://code.google.com/intl/ru/chromium/terms.html>.

Для студентов с ограниченными возможностями здоровья созданы специальные условия для получения образования. Для студентов с ограниченными возможностями здоровья созданы специальные условия для получения образования. Специализированное помещение для инвалидов расположено по адресу: 360004, Кабардино-Балкарская республика, г. Нальчик, ул. Чернышевского, 173, главный учебный корпус университета, аудитория №145.

В целях доступности получения высшего образования по образовательным программам инвалидами и лицами с ограниченными возможностями здоровья университетом обеспечивается:

- альтернативной версией официального сайта в сети «Интернет» для слабовидящих;
- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- для инвалидов и лиц с ограниченными возможностями здоровья по слуху – дублирование в слух справочной информации о расписании учебных занятий; обеспечение надлежащими звуковыми средствами воспроизведения информации;

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).

Лист изменений (дополнений) в рабочей программе дисциплины (модуля)
«Технические средства и методы защиты информации» по направлению подготовки
11.04.01 Радиотехника профиль - Интегрированные системы безопасности с распределенной
архитектурой на 20__ – 20__ учебный год

№ п/п	Элемент (пункт) РПД	Перечень вносимых изменений	Примечание

Обсуждена и рекомендована на заседании кафедры
электроники и цифровых информационных технологий,
 протокол № _____ от « ____ » _____ 20__ г.

Заведующий кафедрой _____ / Р.Ш.Тешев /

дата