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.О.06. ЗАЩИТА 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) «Защита информации» /составители О.Г. Ашхотов, И.Б. Ашхотова, Нальчик, КБГУ, 2023. 19 с.

Рабочая программа дисциплины (модуля) «Защита информации» предназначена для магистров очной формы обучения по направлению подготовки 11.04.01 Радиотехника профиль Интегрированные системы безопасности с распределенной архитектурой, обучающимся в 2 семестре, 1 курса.

Рабочая программа дисциплины (модуля) «Защита информации» составлена с учетом федеральногогосударственногообразовательногостандартавысшегообразованияпонаправлению 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 промежуточной аттестации……. 8
Коллоквиум…….. 8
Вопросы, выносимые на коллоквиум…… 8
Образцы тестовых заданий……. 9
Методические рекомендации по подготовке к тестированию…… 10
Критерии оценивания……. 12
Задания для лабораторных занятий …… 13
6. Промежуточная аттестация…….. 13
7. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности……. 15
8. Учебно-методическое обеспечение дисциплины (модуля)…… 16
Основная литература…… 16
Дополнительная литература…… 16
Интернет-ресурсы…… 16
9. Программное обеспечение современных информационно-коммуникационных технологий……. 16
10. Материально-техническое обеспечение дисциплины…….. 17
Лист изменений (дополнений) в рабочей программе дисциплины (модуля) …… 19

1. Цель и задачи освоения дисциплины(модуля)

Цель курса «Защитаинформации»:изучениетехническихсредствиметодовзащитыинформации автоматизированных систем обработки информации и управления, ремонту и техническому обслуживанию этой аппаратуры. Тенденции и перспективы развития дисциплины определяются центральной проблемой информационных систем – проблемой обеспечения безопасности работы иэксплуатирования.

Основными задачами изучения дисциплины являются следующие представления о:

- видах, источниках и носителях защищаемойинформации;
- классификации техническойразведки;
- методах и средствах инженерной защиты и технической охраныобъектов;
- возможностях видов техническойразведки;
- характеристик государственной системы противодействия техническойразведке;
- основных положений методологии инженерно-технической защитыинформации.

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 от03.07.2019 г. № 480н (зарегистрирован Минюстом России 29.07.2019 г. №55439).

2. Место дисциплины в структуре ОПОПВО

Дисциплина (модуль) «Защита информации» в структуре ОПОП ВО включена в часть обязательных дисциплин Б1.О.06. и изучается магистрами 11.04.01 Радиотехника, профиль Интегрированные системы безопасности с распределенной архитектурой, обучающимся в 2 семестре, 1 курса.

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

- **Эксплуатация радиоэлектронной аппаратуры** (профессиональный стандарт06.005 «Специалист по эксплуатации радиоэлектронных средств (инженер-электроник)», код В, уровень квалификации -5);
- **Разработка единичных технологических процессов и рекомендаций по устранениюипредупреждениюбракавпроизводствеизделиймикроэлектроники**(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 и управления доступом».

3. Требования к результатам освоениядисциплины

Выпускник, освоивший программу магистратуры, должен обладать следующими общепрофессиональными компетенциями:

ОПК-3. Способен приобретать и использовать новую информацию в своей предметной области, предлагать новые идеи и подходы к решению инженерных задач

В результате изучения дисциплины студенты должны:

Знать принципы построения локальных и глобальных компьютерных сетей, основы Интер-

нет-технологий, типовые процедуры применения проблемно-ориентированных прикладных программных средств в дисциплинах профессионального цикла и профессиональной сфере деятельности.

Уметь использовать современные информационные и компьютерные технологии, средства коммуникаций, способствующие повышению эффективности научной и образовательной сфер деятельности.

Владеть методами математического моделирования радиотехнических устройств и систем, технологических процессов с использованием современных информационных технологий.

4.Содержание и структурадисциплины

Содержание разделов дисциплины

Таблица 1

№ Раз-дела	Наименова-ние раздела	Содержание раздела	Код контро-лируе-мой компе-тенции (или ее части)	Форма теку-щего кон-троля
1	Введение	Структура курса. Рейтинговые мероприятия. Реко-мендуемая литература. Цель и задачи курса. Тер-минология, некоторые определения и понятия.	ОПК-3	ЛР, К, РК, Т
2	Основные понятия ин-формаци-оннойбез-опасности	Глобализация инфосферы и связанные с этим угрозы обществу. Основные понятия информаци-онной безопасности. Угрозы и цели защиты инфор-мации. Формы представления информации. Ос-новные направления защиты.	ОПК-3	ЛР, К, РК, Т
3	Методы и средства за-щиты объ-ектов ин-форматиза-ции	Организация защиты информации в РФ. Понятия о видах разведки. Мероприятия по противодействию техническим разведкам. Основные методы добыва-ния информации. Ознакомление с техническими возможностями некоторых средств перехвата ин-формации из помещений, технических средств по эфиру и линиям связи. Физические принципы об-разования каналов утечки и способов защиты ин-формации. Методы и средства защиты информа-ции от утечки из помещений, от технических средств по эфиру и линиям связи. Общие понятия о возможных методах несанкционированного, в том числе деструктивного, воздействия на инфор-мационные ресурсы и оборудование информацион-ных систем. Тактика применения инженерно-тех-нической защиты. Особенности отдельныхмето-дов идентификации и верификации личности.	ОПК-3	ЛР, К, РК, Т

4	Комплексный подход к обеспечению информационной безопасности	Основные положения концепции инженерно-технической защиты информации. 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. Основные понятия информационной безопасности. Угрозы безопасности информации и каналы утечки информации. Комплексный подход к защите информации. Организационная защита информации. Правовое обеспечение информационной безопасности. Инженерно-техническая, криптографическая и программно-аппаратная защита информации.	ОПК-3	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. Разграничение полномочий и управление доступом к ресурсам в защищенных версиях ОС Windows. Стандарты безопасности компьютерных систем и цифровых информационных технологий. Способы симметрического шифрова- ния. Современные алгоритмы симметрического шифрования. Абсолютно стойкий шифр. Прин- ципы создания и свойства асимметрических крип- тосистем. Примеры асимметрических криптоси- стем. Электронная цифровая подпись и ее использование. Функции хеширования. Принципы использования криптографического интерфейса ОС Windows. Компьютерная стеганография и ее применение.	ОПК-3	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.	ОПК-3	ЛР, К, РК, Т
7	Методы физической защиты информации	Методы противодействия наблюдению. Методы противодействия подслушиванию. Экранирование побочных излучений и наводок.	ОПК-3	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.	ОПК-3	ЛР, К, РК, Т

9	Защита от несанкционированного копирования информационных ресурсов	Принципы построения и состав систем защиты от несанкционированного копирования. Методы защиты от копирования инсталляционных дисков и установленного программного обеспечения.	ОПК-3	ЛР, К, РК, Т

Втаблице1приводитсяописаниесодержаниядисциплины,структурированноепоразделам, с указанием по каждому разделу формы текущего контроля: защита лабораторной работы(ЛР),курсовойработы(КР),коллоквиум(К),рубежныйконтроль(РК),тестирование(Т) и т.д.

Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов)

Таблица 2

Вид работы	**Трудоемкость, часы**	
	2 семестр	Всего
Общая трудоемкость (в часах)	**108**	**108**
Контактная работа (в часах):	**51**	**51**
Лекционные занятия (Л)	34	34
Лабораторные работы (ЛР)	17	17
Самостоятельная работа (в часах), в том числе контактная работа:	**48**	**48**
Курсовая работа (КР)/ Курсовой проект (КП)	Не предусмотрены	
Самостоятельное изучение разделов/тем	48	48
Подготовка и прохождение промежуточной аттестации	**9**	**9**
Вид промежуточной аттестации	Зачет	

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.	Системы с разграничением полномочий пользователей на основе паролей.
2.	Программные стандартные и специализированные средства защиты от несанкционированного доступа в защищенных операционных системах.
3.	Блокирование сотовых телефонов. Блокирование Bluetooth и WiFi.
4.	Освоение стандартных и специализированных программных средств защиты от несанкционированного доступа в защищенных операционных системах.
5.	Разработка программы, использующей функции криптографического интерфейса Windows для защиты информации.

6.	Системы с разграничением полномочий пользователей на основе паролей.

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 кибертерроризм.
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 ис-
5	Комплексный подход к защите информации. Организационная защита информации. Правовое обеспечение информационной безопасности. Инженерно-техническая, криптографическая и программно-аппаратная защита информации.
6	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.
7	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.
8	Стандарты безопасности компьютерных систем и цифровых информационных технологий. Спо- собы симметрического шифрования. Современные алгоритмы симметрического шиф- рования. Абсолютно стойкий шифр. Принципы создания и свойстваасимметрических криптосистем. Примеры асимметрическихкриптосистем.
9	Электронная цифровая подпись и ее использование. Функции хеширования. Принципы использования криптографического интерфейса ОС Windows.Компьютерная стеганография и еепримене ние.
10	Побочные электромагнитные излучения и наводки. Технические каналы утечки информации. Методы добывания информации. Методы инженерно-технической защиты
11	Методы противодействия наблюдению. Методы противодействия подслушиванию. Экранирование побочных излучений и наводок.
12	Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и защита от них.

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

5.1.Коллоквиум

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

Вопросы, выносимые на коллоквиум

(контролируемые компетенции ОПК-3)

Первый коллоквиум*(контролируемые компетенции ОПК-3)*

1. Глобализация инфосферы и связанные с этим угрозыобществу.
2. Основные понятия информационной безопасности. Угрозы и цели защитыинформации.

3. Формы представления информации. Основные направлениязащиты.
4. Организация защиты информации в РФ. Понятия о видахразведки.
5. Мероприятия по противодействию техническимразведкам.
6. Основные методы добыванияинформации.
7. Ознакомление с техническими возможностями некоторых средств перехватаинформации из помещений, технических средств по эфиру и линиямсвязи.
8. Физические принципы образования каналов утечки и способов защитыинформации.
9. Методы и средства защиты информации от утечки из помещений, от техническихсредств по эфиру и линиямсвязи.
10. Общие понятия о возможных методах несанкционированного, в том числе деструктивного, воздействия на информационные ресурсы и оборудование информационных систем.
11. Тактика применения инженерно-техническойзащиты.
12. Особенности отдельных методов идентификации и верификациииличности.

Второй коллоквиум *(контролируемые компетенции ОПК-3)*

13. Основные положения концепции инженерно-технической защитыинформации.
14. Теоретические основы инженерно-технической защитыинформации.
15. Характеристика защищаемой информации. Виды, источники и носители защищаемой информации; демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники. Основные понятия информационнойбезопасности.
16. Угрозы безопасности информации и каналы утечки информации. Комплексный подход к защитеинформации.
17. Организационная защита информации. Правовое обеспечение информационнойбезопасности.
18. Инженерно-техническая, криптографическая и программно-аппаратная защита информации.
19. Способы несанкционированного доступа к информации и защиты отнего.
20. Способы аутентификации пользователей компьютерных систем. Протоколы аутентификации при удаленномдоступе.
21. Методы управления доступом к объектам компьютерныхсистем.
22. Средства защиты информации в глобальных вычислительныхсетях.
23. Разграничение полномочий и управление доступом к ресурсам в защищенныхверсиях OCWindows.
24. Стандарты безопасности компьютерных систем и цифровых информационных технологий.

Третий коллоквиум *(контролируемые компетенции ОПК-3)*

25. Способы симметрического шифрования. Современные алгоритмы симметрического шиф- рования. Абсолютно стойкийшифр.
26. Принципы создания и свойства асимметрических криптосистем. Примеры асимметрическихкриптосистем.
27. Электронная цифровая подпись и ее использование. Функциихеширования.
28. Принципы использования криптографического интерфейса OCWindows.
29. Компьютерная стеганография и еепримене ние.
30. Побочные электромагнитные излучения и наводки. Технические каналы утечкиинформации.
31. Методы добывания информации. Методы инженерно-технической защитыинформации.
32. Методы противодействиянаблюдению.
33. Методы противодействия подслушиванию. Экранирование побочных излучений инаводок.
34. Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и защита отних.
35. Принципы построения и состав систем защиты от несанкционированногокопирования.

36. Методы защиты от копирования инсталляционных дисков и установленногопрограммногообеспечения.

Рекомендации при подготовке к коллоквиуму

- проработать конспекты лекций по вопросамколлоквиума;
- прочитать основную и дополнительную литературу, рекомендованную по изучаемымвопросам;
- ответить на вопросыколлоквиума;
- при затруднениях, проконсультироваться спреподавателем.

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 существуизлагает его, не допуская существенных неточностей в ответе навопрос.

5.2. Образцы тестовыхзаданий

(контролируемые компетенцииОПК-3)

1.«Троянский конь» является разновидностью модели воздействия программныхзакладок
искажение
уборка мусора
наблюдение и компрометация
перехват

2.Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные —это
целостность
детерминированность
восстанавливаемость
доступность

3.Достоинствами программной реализации криптографического закрытия данныхявляются
практичность и гибкость
корректность и функциональность
безопасность и эффективность
высокая производительность и простота

4.Достоинством модели конечных состояний политики безопасностиявляется
высокая степень надежности
удобство эксплуатации
дешевизна
простота реализации

5. Единственный ключ используется вкриптосистемах
симметричных
с закрытым ключом

с открытым ключом
асимметричных

6. Кто является основным ответственным за определение уровня классификации информации?
A. Руководитель среднегозвена
B. Высшееруководство
C. Владелец
D. Пользователь

7.Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушениябезопасности?
A. Сотрудники
B. Хакеры
C. Атакующие
D. Контрагенты (лица, работающие подоговору)

8.Если различным группам пользователей с различным уровнем доступа требуется доступк одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
A. Снизить уровень безопасности этой информации для обеспечения ее доступности иудобстваиспользования
B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этойинформации
C. Улучшить контроль за безопасностью этойинформации
D. Снизить уровень классификации этой информации

9. Что самое главное должно продумать руководство при классификацииданных?
A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ кданным
B. Необходимый уровень доступности, целостности иконфиденциальности
C. Оценить уровень риска и отменитьконтрмеры
D. Управление доступом, которое должно защищатьданные

10. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы изащищены?
A. Владельцыданных
B. Пользователи
C. Администраторы
D. Руководство

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)готовяськтестированию,проработатьинформационныйматериалподисциплине.Проконсультироваться с преподавателем по вопросу выбора учебнойлитературы;

б)четковыяснитевсеусловиятестированиязаранее.Знать,сколькотестовВамбудетпредло- жено, 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 опти-

мальный 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	**удовлетвори-тельно 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 лабораторныхзанятий

(контролируемые компетенции ОПК-3)

Лабораторныйпрактикумявляетсяважнымэлементомобучения,т.к.прививаетнавыки самостоятельной работы на различном лабораторном оборудовании и умение пользоваться различными приборами иинструментами.

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. Для этого необходимо подготовиться теоретически. Студенты, не подготовившиеся к работе в соответствии с этими требованиями, к выполнению работы недопускаются.

2. Проведение эксперимента. Этот этап осуществляется в соответствии с методическими указаниями, которые содержатся в описании к каждой работе. Лабораторные работы на персональномкомпьютерестудентможетначатьтолькопослесобеседованияспреподавателеми получения соответствующего допуска. При работе в лаборатории необходимо строго выполнять все правила техники безопасности и указанияпреподавателя.

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

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

- задание;
- теоретическое обоснованиетемы;
- экспериментальныерезультаты;
- общие выводы о работе изаключение.

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 лабораторнаяработа.

6.Промежуточная аттестация

(контролируемые компетенции ОПК-3)

Список основных вопросов к устному зачету

1. Глобализация инфосферы и связанные с этим угрозы обществу. Основные понятия информационной безопасности. Угрозы и цели защитыинформации.

2. Формы представления информации. Основные направления защиты. Организация защиты информации в РФ. Понятия о видах разведки. Мероприятия по противодействию техническимразведкам.
3. Основные методы добывания информации. Ознакомление с техническими возможностями некоторых средств перехвата информации из помещений, технических средств по эфиру и линиямсвязи.
4. Физические принципы образования каналов утечки и способов защиты информации. Методы и средства защиты информации от утечки из помещений, от технических средств по эфиру и линиямсвязи.
5. Общие понятия о возможных методах несанкционированного, в том числе деструктивного, воздействия на информационные ресурсы и оборудование информационных систем.
6. Тактика применения инженерно-техническойзащиты.
7. Особенности отдельных методов идентификации и верификациииличности.
8. Основные положения концепции инженерно-технической защитыинформации.
9. Теоретические основы инженерно-технической защитыинформации.
10. Характеристика защищаемой информации. Виды, источники и носители защищаемой информации; демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники. Основные понятия информационнойбезопасности.
11. Угрозы безопасности информации и каналы утечки информации. Комплексный подход к защитеинформации.
12. Организационная защита информации. Правовое обеспечение информационной безопасности. Инженерно-техническая, криптографическая и программно-аппаратная защита информации.
13. Способы несанкционированного доступа к информации и защиты от него. Способы аутентификации пользователей компьютерных систем. Протоколы аутентификациипри удаленномдоступе.
14. Методы управления доступом к объектам компьютерных систем. Средства защиты информации в глобальных вычислительныхсетях.
15. Разграничение полномочий и управление доступом к ресурсам в защищенныхверсиях OCWindows.
16. Стандарты безопасности компьютерных систем и цифровых информационных технологий.
17. Способы симметрического шифрования. Современные алгоритмы симметрического шифрования. Абсолютно стойкийшифр.
18. Принципы создания и свойства асимметрических криптосистем. Примеры асимметрических криптосистем. Электронная цифровая подпись и ее использование. Функции хеширования.
19. Принципы использования криптографического интерфейса OCWindows.
20. Компьютерная стеганография и еепримене‌ние.
21. Побочные электромагнитные излучения и наводки. Технические каналы утечкиинформации.
22. Методы добывания информации. Методы инженерно-технической защитыинформации.
23. Методы противодействия наблюдению. Методы противодействия подслушиванию.Экранирование побочных излучений инаводок.
24. Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и защита отних.
25. Принципы построения и состав систем защиты от несанкционированного копирования. Методы защиты от копирования инсталляционных дисков и установленного программногообеспечения.

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 защиту.

Для подготовки к ответам вопросы зачета (они выдаются в конце семестра) студент должениспользоватьнетолькокурслекций,ноиосновнуюидополнительнуюлитературудля выработки умения давать развернутые ответы на поставленныевопросы.

Входеподготовкикзачетустудентунеобходимообращатьвниманиенетольконауровеньзапоминания,ноинастепеньпониманияизучаемыхвопросов.Аэтодостигаетсянепростым заучиванием, а усвоением прочных систематизированных знаний аналитическим мышлением. Следовательно, непосредственная подготовка к зачету должна в разумных пропорциях сочетать и запоминание, и понимание программногоматериала.

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 ОПК-3. Указанные компетенции формируются в соответствии со следующими этапами:

- формирование и развитие теоретических знаний, предусмотренных указанными компетенциями (лекционные занятия, самостоятельная работастудентов);
- приобретениеиразвитиепрактическихумений,предусмотренныхкомпетенциями(лабораторные работы, самостоятельная работастудентов);
- закреплениетеоретическихзнаний,уменийипрактическихнавыков,предусмотренных компетенциями (лабораторные работы, практики, выпускная квалификационная работа).

Критерии оценки качества освоения дисциплины, завершающейся зачетом

Баллы (рейтинговой оценки)	**Результат освоения**	**Требования уровню сформированности компетенций**
61-70	Зачтено (без процедуры сдачи зачета)	Обучающийся освоил знания, умения и навыки, входящие в состав компетенций: Способен приобретать и использовать новую информацию в своей предметной области, предлагать новые идеи и подходы к решению инженерных задач (ОПК-3)

36-61	Зачтено (с процедурой сдачи зачета)	Обучающийся проявляет компетенции ОПК-3, 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.

Приответеобучающийсяможетдопуститьнекоторыенеточности,негрубыеошибки,затрудняться в самостоятельном изложении материала, но правильно отвечать на задаваемые ему вопросы, в результате наводящих вопросов с помощью преподавателя исправлять допущенные ошибки инеточности.

«Незачтено»можетбытьвыставленообучающемуся,обнаружившемунеполное,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 профессиональнойдеятельности.

7.Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опытадеятельности

Результаты освоения учебной дисциплины, подлежащие проверке.

Таблица 6.

Результаты обучения (компетенции)	Основные показатели оценки результатов обучения	Вид оценочного материала
ОПК-3. Способен приобретать и использовать новую информацию в своей предметной области, предлагать новые идеи и подходы к решению инженерных задач **Код и наименование индикатора достижения компетенции: ОПК-М.3.1.**Способен использовать новую информацию и программные средства в дисциплинах профессиональной деятельности	***Знает:*** принципы построения локальных и глобальных компьютерных сетей, основы Интернет-технологий, типовые процедуры применения проблемно-ориентированных прикладных программных средств в дисциплинах профессионального цикла и профессиональной сфере деятельности	Выполнение и защита лабораторных работ; типовые оценочные материалы для устного опроса ***(раздел 5.1.1);*** типовые тестовые задания ***(раздел5.2.);*** типовые оценочные материалы ***(раздел 6.).***
	Умеет: использовать современные ин- формационные и компьютерные техно- логии, средства коммуникаций, способствующие повышению эффективности научной и образовательной сфер деятельности	Выполнение и защита лабораторных работ; типовые оценочные материалы для устного опроса ***(раздел 5.1.1);*** типовые тестовые задания ***(раздел5.2.);*** типовые оценочные материалы ***(раздел 6.).***

ОПК-М.3.2. Приобретает с помощью ин- формационных технологий новые знаниявсвоейпредмет-нойобласти.	***Владеет:*** методами математического моделирования радиотехнических устройств и систем, технологических процессов с использованием современ- ных информационных технологий	Выполнение и защита лабораторных работ; типовые оценочные материалы для устного опроса ***(раздел 5.1.1);*** типовые тестовые задания ***(раздел5.2.);*** типовые оценочные материалы ***(раздел 6.).***

7.Учебно-методическое обеспечениедисциплины

Основная литература

1. Каторин Ю.Ф. Защита информации техническими средствами. (Электронный ресурс) – СПб.: Ун-т ИТМО. 2012.http://www.iprbookshop.ru/66445.html
2. Башлы П.Н. Информационная безопасность и защита информации. (Электронныйресурс) –М. Евразийский открытый ин-т. 2012. http://iprbookshop.ru/10677.html
3. Ерохин В.В. Безопасность информационных систем (Электронный ресурс) –М.: ФЛИНТА, 2015.http://www.studentlibrary.ru/book/ISBN9785976519046html
4. Оверченков В.И. и др. Методы и средства инженерно-технической защиты информации. (Электронный ресурс) – Брянск: Брянский гос. тех. ун-т.2012.http://iprbookshop.ru/7000.html
5. Котова Л.В. Методы и средства защиты информации. –М.: МГУ.2015.

Дополнительная литература:

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Техническая защита информации. Учебник для ВУЗов. Гриф УМО ВУЗов России. 5-е изд. – М.: Горячая линия – Телеком,2009. – 616 с.
2. Зайцев А.П. Технические средства обеспечения информационной безопасности. Часть 1. Технические каналы утечки информации. Учебное пособие.- Издание 2-ое переработанное и дополненное. - Томск: В-Спектр, 2007.-200с.
3. Зайцев А.П. Технические средства обеспечения информационной безопасности. Часть 2. Средства защиты информации от утечки по техническим каналам. Учебное пособие.- Издание 2-ое переработанное и дополненное. - Томск: В-Спектр, 2007.-280с.
4. Зайцев А.П., Шелупанов А.А. Технические средства и методы защиты информации. Лабораторный практикум. Гриф СибРОУМО. - Томск: В-Спектр,2007.-120с.
5. Зайцев А.П., Шелупанов А.А. Практикум по техническим средствам и методам защиты информации. Учебное пособие. Гриф СибРОУМО. Издание 2-е, исправленное и дополненное. - Томск: Изд-во "В-Спектр",2007.-128с.

Периодические издания

Перечень периодических изданий, получаемых библиотекой КБГУ, в которых студент можетознакомитьсяссовременнымидостижениямивобластиосновзащитыинформации:Журнал «Алгоритм безопасности», Технологии защиты, Безопасность, Мониторинг. Наука и безопасность.

Интернет-ресурсы

http://lib.kbsu.ru/- Библиотека КБГУ.
http://www.garant.ru/- Справочная правовая система «Гарант».
http://www.consultant.ru/-Справочная правовая система «КонсультантПлюс».
http://www.ph4s.ru/book_electronika.html- Образовательный проект А.Н. Варгина
http://www.Russianelectronics.ru-портал «Время электроники»;
https://www.sciencedirect.com/- Полнотекстовая база данныхScienceDirect.
http://www.analitika.infoСредства защиты информации. Каталог техники выявления и противодействия средствам разведки, антитеррора. Форум по вопросам защиты информации.
http://www.radioscanner.ruСайт по радиомониторингу и профессиональной радиосвязи. Каталог радиоприемников,радиостанций.

http://www.inside-zi.ruСайт журнала "Защита информации. Инсайд". На сайте можно ознакомиться с содержанием журналов как готовящихся к выходу, так и прошлых лет.
http://www.analitika.infoСредства защиты информации. Каталог техники выявления и противодействия средствам разведки, антитеррора. Форум по вопросам защиты информации.
http://www.radioscanner.ruСайт по радиомониторингу и профессиональной радиосвязи. Каталог радиоприемников,радиостанций.
http://www.inside-zi.ruСайт журнала "Защита информации. Инсайд". На сайте можно ознакомиться с содержанием журналов как готовящихся к выходу, так и прошлых лет.

9. Программное обеспечение современных информационно-коммуникационныхтехнологий

1. Студентыимеютдоступкединомуобразовательномупорталу,гдемогутвоткрытом доступе пользоваться ресурсами учебно-методической литературы, являющимися разработками ведущих ВУЗОВРоссии.

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

3. При выполнении лабораторного практикума студенты работают в ОС Windows10, языках программирования Делфи, С++.

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

10.Материально-техническое обеспечение дисциплины

Материально-техническую базу для проведения занятий по дисциплине составляют:

- специализированная аудитория, используемая при проведении занятий лекционного типа №134, расположенная по адресу: 360004, Кабардино-Балкарская республика, г. Нальчик, ул. Чернышевского, 175, условный номер - 14, оснащенная мультимедийным проектором и комплектом аппаратуры, позволяющей демонстрировать текстовые и графическиематериалы;
- рабочее место преподавателя;
- рабочие местастудентов;
- меловаядоска.

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

Дисциплина обеспечена:

- тестовымматериаламивэлектроннойобучающейсистеме«Moodle»(Открытый университет);
- книжным фондомбиблиотеки;
- электронными версиями лекций иучебников.

Лабораторные занятия проводятся в лаборатории №129, расположенной по адресу: 360004, Кабардино-Балкарская республика, г. Нальчик, ул. Чернышевского, 175, условный номер-14.Лабораторияоснащенаперсональнымикомпьютерамиинеобходимымпрограммным обеспечением.

Студенты имеют доступ через Интернет доступ к электронной обучающей системе «Moodle»(Открытыйуниверситет),котораяпозволяетразмещатьэлектронныеучебныекурсы в свободном доступе для студентовуниверситета.

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 адресуhttps://www.adobe.com/ru/legal/terms.html;
- Mozilla Firefox лицензия: GPL/LGPL/MPL, Google Chromелицензия:предоставляется бесплатнонаусловияхлицензионныхсоглашенийнапрограммноеобеспечениесот- крытым исходным кодом по адресуhttps://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 ограниченнымивозможностями здоровья университетом обеспечивается:

- альтернативной версией официального сайта в сети «Интернет» дляслабовидящих;
- присутствие ассистента, оказывающего обучающемуся необходимуюпомощь;
- дляинвалидовилицсограниченнымивозможностямиздоровьяпослуху–дублированиевслухсправочнойинформациирасписанииучебныхзанятий;обеспечениенадлежащими звуковыми средствами воспроизведенияинформации;

для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательногоаппарата,созданыматериально-техническиеусловия,обеспечивающие возможностьбеспрепятственногодоступаобучающихсявучебныепомещения,объектупитания, туалетные и другие помещения университета, а также пребывания в указанных помещениях (наличие расширенных дверных проемов, поручней и другихприспособлений).

Лист изменений (дополнений)в рабочей программе дисциплины (модуля)
«Защита 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