Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

РЕКОМЕНДОВАНО
К УТВЕРЖДЕНИЮ
Декан, председатель совета
факультета КТВТиЭ
_____ **Ш. А. Юсуфов**
«18» 10 **2018 г.**

УТВЕ́РЖДАЮ
Проректор по учебной работе,
председатель методического
совета ДГТУ
_____ **Н. С. Суракатов**
«21» 10 **2018 г.**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина С1.Б.27 Техническая защита информации

для специальности 10.05.03-«Информационная безопасность автоматизированных систем»

специализация «Безопасность открытых информационных систем»

факультет «Компьютерных технологий, вычислительной техники и энергетики»
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника (степень) Специалист по защите информации
бакалавр (специалист)

Форма обучения очная : курс4: семестр 8:

Всего трудоемкость в зачетных единицах (часах) 4 ЗЕТ (144 часа)

Лекции 34 (час); зачет 8 семестр

практические (семинарские) занятия - (час): экзамен - (семестр)

лабораторные занятия 34 (час): самостоятельная работа 76 (час);

курсовой проект (работа, РГР)-(семестр).

Зав. кафедрой ИБ _____ Г.И. Качаева
подпись

Начальник УО _____ Э.В. Магомаева
подпись

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем».

Программа одобрена на заседании выпускающей кафедры ИБ от 15.10.2018г., протокол № 2

Зав. выпускающей кафедрой по данной специальности _____ **Г.И. Качаева**

ОДОБРЕНО
Методической комиссией по укрупненным группам специальностей и направлению подготовки
10.00.00- «Информационная безопасность»
Председатель МК
_____ Мелехин В.Б.
подпись ИОФ

«15» 10 2018г.

АВТОР ПРОГРАММЫ

Качаева Г.И., к.э.н., ст. преп. каф. ИБ
И.О.Ф. уч. степень, ученое звание, подпись

_____

1. Цели и задачи дисциплины

1.1 **Цели дисциплины**

Цель дисциплины - формирование знаний в области принципов добывания (разведки) информации, способов организационно-технической и технической защиты информации, активных и пассивных способов и средств скрытия и защиты, способов и средств технической дезинформации, принципов технического контроля защищенности объектов.

1.2 Задачи дисциплины

Задачи изучения дисциплины:

- изучение систем и средств инженерно-технической разведки, методов и способов организации защиты объектов активными и пассивными способами и техническими средствами, выбора оптимальных (по условиям эксплуатации и экономичности) технических средств защиты информации, нормативно-методических и правовых документов, регламентирующих вопросы технической защиты информации;
- формирование умения выявлять каналы утечки на конкретных объектах и оценивать их возможности;
- формирование умения определять рациональные меры защиты на объектах и оценивать уровень эффективности их защиты;

2. Место дисциплины в структуре ООП специалитета

Дисциплина «Техническая защита информации» относится к базовой части ФГОС ВО.

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: языки программирования.

Последующими дисциплинами являются: Защита программ и данных

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующей компетенции:

способностью проводить анализ защищенности автоматизированных систем (ПК-3);

способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);

способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);

способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17).

В результате изучения дисциплины студент должен

Знать:

- Концепцию инженерно-технической защиты информации.
- Нормативно-правовые документы обеспечения информационной безопасности.
- Технические каналы утечки информации.
- Физические принципы утечки информации по техническим каналам.
- Методы обнаружения и защиты информации в технических каналах от ее утечки.

Уметь:

- Применять методы инженерно-технической защиты информации.
- Анализировать возможные уязвимые места технической защиты информации.
- Проводить предварительный сбор данных о технических уязвимостях.
- Проектировать системы защиты и проводить анализ рисков утечки информации по техническим каналам.

Владеть:

- навыками работы с программным обеспечением по оценки рисков утечки информации по техническим каналам и программно-аппаратными комплексами по выявлению каналов утечки информации.

4. Структура и содержание дисциплины «Техническая защита информации»

Общая трудоемкость дисциплины составляет 4 зачетные единицы – 144 часов, в том числе: лекционных -34 часа, лабораторных - 34 часа, СРС – 76 часов, форма отчетности зачет в 8 семестре.

4.1.Содержание дисциплины

	Раздел дисциплины Тема лекции и вопросы	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего* контроля успеваемости *(по срокам текущих аттестаций в семестре)*
				ЛК	ПЗ	ЛР	СР	
1.	**Лекция №1** **Тема: «Характеристика технических каналов утечки информации»** Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации. Каналы утечки речевой информации.	5	1	2		2	4	Вх. Контр.
2.	**Лекция № 2** **Тема: «Характеристика технических каналов утечки информации»** Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники.		2	2		2	4	
3.	**Лекция № 3** **Тема: «Средства обнаружения каналов утечки информации»** Индикаторы электромагнитных излучений. Радиочастотомеры.		3	2		2	4	
4.	**Лекция № 4** **Тема: «Средства обнаружения каналов утечки информации»** Нелинейные локаторы. Досмотровая техника		4	2		2	4	
5.	**Лекция № 5** **Тема: «Организация инженерно-технической защиты информации»** Организационно-методические основы защиты информации. Общие требования к защите информации.		5	2		2	4	АКР №1
6.	**Лекция № 6** **Тема: «Организация инженерно-технической защиты информации»** Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации		6	2		2	4	
7.	**Лекция № 7** **Тема: «Методы и средства защиты информации»** Организация защиты речевой информации. Пассивные средства защиты выделекнных помещений. Аппаратура и способы активной защиты помещений от утечки речевой информации.		7	2			4	

8.	**Лекция № 8** **Тема: «Методы и средства защиты информации»** Рекомендации про выбору систем виброакустической защиты. Подавление диктофонов. Нейтрализация радиомикрофонов. Защита электросети. Защита оконечного оборудования слаботочных линий. Защита абонентского участка телефонных линий.		8	2		2	4	
9.	**Лекция № 9** **Тема: «Организация защиты информации»** Организация защиты информации от утечки возникающей при работе вычислительной техники за счет ПЭМИН. Методология защиты информации от утечки за счет ПЭМИН.		9	2		2	6	
10.	**Лекция № 10** **Тема: «Организация защиты информации»** Критерий защищенности средств вычислительной техники. Нормированные уровни помех в каналах утечки. Методика проведения специальных исследований технических средств ЭВТ.		10	2		2	4	АКР №2
11.	**Лекция № 11** **Тема: «Мероприятия по выявлению каналов утечки информации»** Специальные проверки. Порядок проведения специальной проверки технических средств		11	2		2	4	
12.	**Лекции № 12** **Тема: «Каналы утечки информации»** Специальные обследования. Подготовка к проведению специальных обследований.	8	12	2		2	6	
13.	**Лекции № 13** **Тема: «Каналы утечки информации»** Выполнение поисковых мероприятий. Подготовка отчетных материалов.		13	2		2	4	
14.	**Лекция № 14** **Тема: «Методы отладки и тестирования программ»** Категории программных ошибок. Типы тестов. Тестирование на этапе планирования. Тестирование на этапе проектирования.		14	2		2	4	
15.	**Лекция № 15** **Тема: «Методы отладки и тестирования программ»** Тестирование " белого ящика" на стадии кодирования. Регрессионное тестирование. Тестирование "черного ящика". Разработка тестов.		15	2		2	6	АКР №3
16.	**Лекция № 16** **Тема: «Общая характеристика алгоритмов сжатия данных»** Алгоритм построения кода Шеннона-Фано. Код Хаффмана. Построение кодового дерева. Обратимое и необратимое сжатие.		16	2		2	6	
17.	**Лекция № 17** **Тема: «Общая характеристика алгоритмов**		17	2		2	4	

	сжатия данных» Сжатие данных методом кодирования серий. Особенности арифметического кодирования.							
	Итого по дисциплине			**34**		**34**	**76**	**зачет**

4.2. Содержание лабораторных занятий

№ п/п	№ лекции израбочей программы	Наименование лабораторных заняти1	Рекомендуемая литература и методические разработки (№ источника из списка литературы)	Кол-во часов
1	Лк №1	Тема: «Характеристика технических каналов утечки информации»	№№ 1-8	2
2	Лк №2	Тема: «Характеристика технических каналов утечки информации»	№№ 1-8	2
3	Лк №3	Тема: «Средства обнаружения каналов утечки информации»	№№ 1-8	2
4	Лк № 4	Тема: «Средства обнаружения каналов утечки информации»	№№ 1-8	2
5	Лк № 5	Тема: «Организация инженерно-технической защиты информации»	№№ 1-8	2
6	Лк №6	Тема: «Организация инженерно-технической защиты информации»	№№ 1-8	2
7	Лк № 7	Тема: «Методы и средства защиты информации»	№№ 1-8	2
8	Лк №8	Тема: «Методы и средства защиты информации»	№№ 1-8	2
9	Лк №9	Тема: «Организация защиты информации»	№№ 1-8	2
10	Лк №10	Тема: «Организация защиты информации»	№№ 1-8	
11	Лк №11	Тема: «Мероприятия по выявлению каналов утечки информации»	№№ 1-8	2
12	Лк №12	Тема: «Каналы утечки информации»	№№ 1-8	2
13	Лк №13	Тема: «Каналы утечки информации»	№№ 1-8	2
14	Лк №14	Тема: «Методы отладки и тестирования программ»	№№ 1-8	2
15	Лк №15	Тема: «Методы отладки и тестирования программ»	№№ 1-8	2
16	Лк №16	Тема: «Общая характеристика алгоритмов сжатия данных»	№№ 1-8	2
17	Лк №17	Тема: «Общая характеристика алгоритмов сжатия данных»	№№ 1-8	2
Итого по дисциплине				**34**

4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Кол-во часов из содержания дисциплины	Рекомендуемая литература и источники информации	Формаконтроля СРС
1.	Тема: «Характеристика технических	4	№№ 1-8	Опрос, реферат,

	каналов утечки информации»			статья
2.	Тема: «Характеристика технических каналов утечки информации»	4	№№ 1-8	Опрос, реферат, статья
3.	Тема: «Средства обнаружения каналов утечки информации»	4	№№ 1-8	Опрос, реферат, статья
4.	Тема: «Средства обнаружения каналов утечки информации»	4	№№ 1-8	Опрос, реферат, статья
5.	Тема: «Организация инженерно-технической защиты информации»	4	№№ 1-8	Опрос, реферат, статья
6.	Тема: «Организация инженерно-технической защиты информации»	4	№№ 1-8	Опрос, реферат, статья
7.	Тема: «Методы и средства защиты информации»	4	№№ 1-8	Опрос, реферат, статья
8.	Тема: «Методы и средства защиты информации»	4	№№ 1-8	Опрос, реферат, статья
9.	Тема: «Организация защиты информации»	6	№№ 1-8	Опрос, реферат, статья
10.	Тема: «Организация защиты информации»	4	№№ 1-8	
11.	Тема: «Мероприятия по выявлению каналов утечки информации»	4	№№ 1-8	
12.	Тема: «Каналы утечки информации»	6	№№ 1-8	
13.	Тема: «Каналы утечки информации»	4	№№ 1-8	
14.	Тема: «Методы отладки и тестирования программ»	4	№№ 1-8	
15.	Тема: «Методы отладки и тестирования программ»	6	№№ 1-8	
16.	Тема: «Общая характеристика алгоритмов сжатия данных»	6	№№ 1-8	
17.	Тема: «Общая характеристика алгоритмов сжатия данных»	4	№№ 1-8	
Итого		**76**		

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по специальности реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и в целом в учебном процессе они составляют не менее 20% аудиторных занятий.

При проведении занятий по учебной дисциплине рекомендуется следовать и традиционным технологиям, в частности, в каждом разделе курса выделять наиболее важные моменты, акцентировать на них внимание обучаемых.

При чтении лекций по всем разделам программы иллюстрировать теоретический материал большим количеством примеров, что позволит сделать изложение наглядным и продемонстрировать обучаемым приемы программирования.

При изучении всех разделов программы добиться точного знания обучаемыми основных исходных понятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно– методическое обеспечение самостоятельной работы студентов

Вопросы входного контроля для проверки знаний студентов

1. Что такое программное обеспечение?
2. Жизненный цикл программного обеспечения.
3. Модели разработки программного обеспечения
4. Объектно-ориентированный подход.
5. Модель «водопада» разработки программного обеспечения.
6. Определение, краткая характеристика. Агрегацией и композиция классов.
7. Понятия и соотношение. Интерфейсы. Проектирование классов. Структура класса.
8. Диаграммы состояний объекта. Способы проектирование методов класса. Парадигмы программирования: визуальная, функциональная, процедурная, объектно-ориентированная и т.д.
9. Объектно-ориентированная парадигма: понятия объекта, класса объектов; основные понятия объектно-ориентированного программировании (инкапсуляция, наследование и поли- морфизм); классы и объекты; интерфейсы и реализация.

Контрольные вопросы для проверки текущих знаний студентов
Аттестационная контрольная работа №1

1. Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации.
2. Каналы утечки речевой информации.
3. Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники.
4. Индикаторы электромагнитных излучений.
5. Радиочастотомеры.
6. Нелинейные локаторы.
7. Досмотровая техника
8. Организационно-методические основы защиты информации.
9. Общие требования к защите информации.
10. Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации

Аттестационная контрольная работа №2

1. Организация защиты информации от утечки возникающей при работе вычислительной техники за счет ПЭМИН.
2. Методология защиты информации от утечки за счет ПЭМИН.
3. Критерий защищенности средств вычислительной техники.
4. Нормированные уровни помех в каналах утечки.
5. Методика проведения специальных исследований технических средств ЭВТ.

Аттестационная контрольная работа №3

1. Специальные проверки.
2. Порядок проведения специальной проверки технических средств
3. Специальные обследования.
4. Подготовка к проведению специальных обследований.
5. Выполнение поисковых мероприятий.
6. Подготовка отчетных материалов.
7. Категории программных ошибок.
8. Типы тестов. Тестирование на этапе планирования.
9. Тестирование на этапе проектирования.
10. Тестирование "белого ящика" на стадии кодирования.
11. Регрессионное тестирование. Тестирование "черного ящика".
12. Разработка тестов.

Перечень вопросов на зачет

1. Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации.
2. Каналы утечки речевой информации.
3. Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники.
4. Индикаторы электромагнитных излучений.
5. Радиочастотомеры.
6. Нелинейные локаторы.
7. Досмотровая техника
8. Организационно-методические основы защиты информации.
9. Общие требования к защите информации.
10. Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации
11. Организация защиты информации от утечки возникающей при работе вычислительной техники за счет ПЭМИН.
12. Методология защиты информации от утечки за счет ПЭМИН.
13. Критерий защищенности средств вычислительной техники.
14. Нормированные уровни помех в каналах утечки.
15. Методика проведения специальных исследований технических средств ЭВТ.
16. Специальные проверки.
17. Порядок проведения специальной проверки технических средств
18. Специальные обследования.
19. Подготовка к проведению специальных обследований.
20. Выполнение поисковых мероприятий.
21. Подготовка отчетных материалов.
22. Категории программных ошибок.
23. Типы тестов. Тестирование на этапе планирования.
24. Тестирование на этапе проектирования.
25. Тестирование "белого ящика" на стадии кодирования.
26. Регрессионное тестирование. Тестирование "черного ящика".
27. Разработка тестов.

.

Вопросы проверки остаточных знаний

1. Структуры данных
2. Динамические структуры данных
3. Деревья
4. Алгоритмы
5. Алгоритмы на графах
6. Алгоритмы сортировки
7. Алгоритмы поиска
8. Технологии проектирования и программирования
9. Объектно-ориентированный подход к разработке ПО
10. Технология создания программного кода»
11. Технологии коллективной разработки программного обеспечения
12. Технологические средства разработки программного обеспечения
13. Методы отладки и тестирования программ
14. Документирование и оценка качества программных продуктов

7. Учебно-методическое и информационное обеспечение дисциплины (модуля) «Техническая защита информации»

7.1. Рекомендуемая литература и источники информации

Зав. библиотекой _____

№	Виды заня-тий (лк, пр, лб, срс)	Комплект необходимой учебной лит-ры по дисциплинам (наименование учебника, пособия)	Авторы	Издат-во и год издания	Кол-во пособий, учебников и прочей литер-ры	
ОСНОВНАЯ					в библ	на каф
1.	Лк, лб, срс	Теория информации и кодирования	Санников В.Г..	Московский технический университет связи и информатики, 2015.— 95 с	http://www.iprbookshop.ru/61558	
2.	Лк, пр, срс	Информационная безопасность и защита информации	Шаньгин, В. Ф.	Электрон. текстовые дан. – Москва : ДМК Пресс, 2014. – 702 с	http://www.iprbookshop.ru/29257	
3.	Лк, пр, срс	Универсальное кодирование. Теория и алгоритмы	Штарьков, Ю. М.	Электрон. текстовые дан. – Москва : ФИЗМАТЛИТ, 2013. – 280 с	http://www.iprbookshop.ru/24451	
ДОПОЛНИТЕЛЬНАЯ						
4.	Лк, лб, срс	Технологии программирования. Компонентный подход [Электронный ресурс	Кулямин, В. В.	М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 590 с. — 5-9556-0067-1.	http://www.iprbookshop.ru/73733.html	
5.	Лк, лб, срс	Методические указания к практическим занятиям и самостоятельной работы по дисциплине «Технологии и методы программирования».	Г.И. Качаева	Махачкала: ФГБОУ ВПО «ДГТУ» ,2014	-	30
6.	ЛК,СР, КР	http://dstu.ru/nauka/biblioteka/ – образовательный портал университета				
7.	ЛК,СР, КР	http://www.elibrary.ru – научная электронная библиотека				
8.	ЛК,СР, КР	http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.				

7.2. Программное обеспечение

Интегрированные среды разработки программ Borland Developer Studio и Visual Studio . NET, базы данных, информационно – справочные и поисковые системы; вузовские электронно-библиотечные системы учебной литературы; база научно-технической информации ВИНИТИ РАН.

8. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий и лабораторного практикума на основе интерактивных методов обучения необходим доступ в Интернет из компьютерного зала, наличие цифрового проектора для применения современных обучающих мультимедиа – технологий.

Программное обеспечение:

- операционная система Microsoft Windows;
- текстовый процессор Microsoft Word;
- web-браузер;
- среда программирования.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03- «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем».

Рецензент от выпускающей кафедры (работодателя) по специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем».

подпись

З.Ф. Рагимова

ФИО