


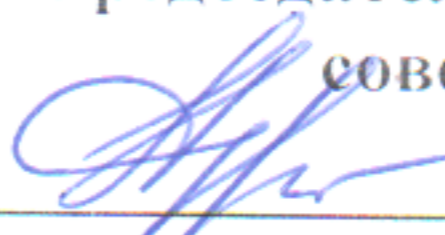
Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

РЕКОМЕНДОВАНО
К УТВЕРЖДЕНИЮ
Декан, председатель совета
факультета КТВТиЭ


Ш. А. Юсуфов
« 17 » 10 20 18 г.

УТВЕРЖДАЮ

Проректор по учебной работе,
председатель методического
совета ДГТУ


Н. С. Суракатов
« 22 » 10 20 18 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина С1.В.ОД.9 Комплексное обеспечение информационной безопасности автоматизированных систем

Специальность 10.05.03 – Информационная безопасность автоматизированных систем

Факультет Компьютерных технологий, вычислительной техники и энергетики
наименование факультета, где ведется дисциплина

Кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника Специалист по защите информации

Форма обучения очная; курс 4; семестр 8;

Всего трудоемкость в зачетных единицах (часах) 53ЕТ (180 ч)

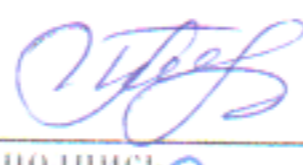
Лекции 34 (час); зачет 8

практические (семинарские) занятия - (час); экзамен 8 (1 зет=36ч) (семестр)

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

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

Зав. кафедрой ИБ


подпись

Г.И. Качаева

Начальник УО


подпись

Э.В. Магомаева



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 данному направлению  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 у студентов знаний по организационным мероприятиям по защите информации, а также навыков и умения в применении знаний для конкретных условий.

1.2 Задачи дисциплины

Задачи изучения дисциплины:

- о предотвращении и расследовании компьютерных преступлений;
- об угрозах информационной безопасности объекта;
- об организации службы безопасности объекта;
- о подборе и работе с кадрами в сфере информационной безопасности;
- об организации и обеспечении режима секретности;
- об охране объектов.

2. Место дисциплины в структуре ООП специалитета

Дисциплина «Комплексное обеспечение информационной безопасности автоматизированных систем» относится к вариативной 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: ПК-5, ПК-8, ПК-11, ПК-12, ПК-13, ПК-14, ПК-17

- способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);
- способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);
- способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);
- способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);
- способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);
- способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);
- способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17).

В результате изучения дисциплины студент должен

Знать:

- концептуальные основы комплексного обеспечения информационной безопасности автоматизированных систем;
- общие методологические принципы комплексных системы обеспечения информационной безопасности;
- основные методы и средства проектирования систем обеспечения информационной безопасности;
- методы оценки качества систем и моделей; об определении и измерении параметров опасных сигналов для технических каналов утечки информации и определять эффективность защиты от утечки информации.

Уметь:

- выявлять возможные способы нарушения информационной безопасности при работе автоматизированных систем обработки информации;
- применять стандартные криптографические решения для защиты информации и квалифицированно оценивать их качество;
- оценивать модели и политику безопасности;
- реализовывать системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем.

Владеть навыками:

- практически решать задачи защиты программ и данных программно-аппаратными средствами и давать оценку качества предлагаемых решений;
- применять системный подход к обеспечению информационной безопасности в различных сферах деятельности;
- проектировать и реализовывать комплексную систему защиты информации, оценивать ее качество.

3. Структура и содержание дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем»

Общая трудоемкость дисциплины составляет 5 зачетных единиц – 180 часов, в том числе: лекционных -34 часов, лабораторных - 34 часа, СРС – 76 часов, форма отчетности зачет и экзамен в 8 семестре.

4.1.Содержание дисциплины

№ п/п	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	
	Лекция №1 Тема: «Место организационного обеспечения информационной безопасности в системе комплексной защиты информации» Информационная сфера и информационная среда. Виды защищаемой информации.	8	1,2	4		2	7	Вх. Контр.
1.	Лекция №2 Тема: «Анализ и оценка угроз информационной безопасности информационной системы» Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации. Виды угроз информационной безопасности объекту защиты и их характеристика. Модель нарушителя информационной безопасности. Модель угрозы информационной безопасности.		3,4	4		2	7	
2.	Лекция № 3 Тема: «Организационные источники и каналы утечки информации» Структура сил и средств организационной защиты информации. Функции, задачи и особенности службы безопасности организации. Принципы организации службы безопасности организации. Типовая структура службы безопасности. Основные документы, регламентирующие деятельность службы безопасности объекта. Участие сотрудников в организационной защите информации. Взаимодействие службы безопасности объекта с правоохранительными органами.		5,6	4		2	7	АКР №1

3.	<p>Лекция №4 Тема: «Организация и обеспечение режима секретности»</p> <p>Обеспечение режима секретности при проведении НИОКР по секретной (конфиденциальной) тематике, при разработке и изготовлении изделий, их опытной эксплуатации и серийном производстве. Требования режима секретности при работе с секретными документами. Назначение и задачи секретного делопроизводства. Порядок разработки, учета, хранения, размножения и уничтожения секретных (конфиденциальных) документов. Понятия допуска к секретной (конфиденциальной) информации и доступа к (конфиденциальным) работам, документам и изделиям. Формы допусков. Служебное расследование нарушений режима секретности. Организация работ по защите информации при опубликовании открытых материалов.</p>		7,8	4		2	7	
4.	<p>Лекция № 5 Тема: «Архитектура систем защиты информации»</p> <p>Подсистема контроля доступа и аудита. Подсистема администрирования безопасности.</p>		9,10	4		2	7	АКР№2
5.	<p>Лекция № 6 Тема: «Организация и обеспечение работ по защите информации»</p> <p>Назначение и требования внутриобъектового режима. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации. Требования к помещениям, в которых циркулирует защищаемая информация. Понятие пропускного режима. Цели и задачи пропускного режима. Организация пропускного режима. Атрибутные и биометрические идентификаторы людей. Порядок оформления и выдачи пропусков.</p>		11,12	4		2	8	
6.	<p>Лекции № 7 Тема: «Методы оценки безопасности информации на объектах ее обработки»</p> <p>Оценка ущерба и анализ рисков информационной безопасности. Оценка затрат на организацию и проведение мероприятий по обеспечению информационной безопасности.</p>	8	13,14	4		2	8	

7.	<p>Лекция №8 Тема: «Организация защиты информации при осуществлении международного сотрудничества» Порядок организации информационной безопасности объекта при осуществлении международного научнотехнического и экономического сотрудничества. Основные требования, предъявляемые к подготовке служебного совещания. Организация обеспечения режима секретности при проведении служебного совещания. Требования к помещениям для проведения совещания</p>	15,16	4	2	8	АКР№ 3
8.	<p>Лекция №9 Тема: «Защита каналов связи в Интернет» Виды используемых в Интернет каналов связи. Особенности их защиты. Использование межсетевых экранов. Виртуальные частные сети.</p>	17	2		7	
	Итого по дисциплине		34	34	76	Зачет, Экзамен (Зет=36ч)

4.2. Содержание лабораторных занятий

№ п/п	№ лекции израбочей программы	Наименование лабораторного (практического, семинарского) занятия	Рекомендуемая литература и методические разработки (№ источника из списка литературы)	Кол-во часов
1	Лк №1	Тема: «Место организационного обеспечения информационной безопасности в системе комплексной защиты информации»	№№ 1-9	4
2	Лк №2	Тема: «Анализ и оценка угроз информационной безопасности информационной системы»	№№ 1-9	4
3	Лк №3	Тема: «Организационные источники и каналы утечки информации»	№№ 1-9	4
4	Лк № 4	Тема: «Организация и обеспечение режима секретности»	№№ 1-9	4
5	Лк № 5	Тема: «Архитектура систем защиты информации»	№№ 1-9	4
6	Лк №6	Тема: «Организация и обеспечение работ по защите информации»	№№ 1-9	4
7	Лк № 7	Тема: «Методы оценки безопасности информации на объектах ее обработки»	№№ 1-9	4
8	Лк №8	Тема: «Организация защиты информации при осуществлении международного сотрудничества»	№№ 1-9	4
9	Лк№9	Тема: «Защита каналов связи в Интернет»	№№ 1-9	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 сопровождения	Рекомендуем ая литература и источники информации	Форма контро ля СРС
1.	Тема: «Место организационного обеспечения информационной безопасности в системе комплексной защиты информации»	7	№№ 1-9	Опрос, реферат, статья
2.	Тема: «Анализ и оценка угроз информационной безопасности»	7	№№ 1-9	Опрос, реферат, статья

	информационной системы»			
3.	Тема: «Организационные источники и каналы утечки информации»	7	№№ 1-9	Опрос, реферат, статья
4.	Тема: «Организация и обеспечение режима секретности»	7	№№ 1-9	Опрос, реферат, статья
5.	Тема: «Архитектура систем защиты информации»	7	№№ 1-9	Опрос, реферат, статья
6.	Тема: «Организация и обеспечение работ по защите информации»	8	№№ 1-9	Опрос, реферат, статья
7.	Тема: «Методы оценки безопасности информации на объектах ее обработки»	8	№№ 1-9	Опрос, реферат, статья
8.	Тема: «Организация защиты информации при осуществлении международного сотрудничества»	8	№№ 1-9	Опрос, реферат, статья
9.	Тема: «Защита каналов связи в Интернет»	7	№№ 1-9	Опрос, реферат, статья
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 программирования (инкапсуляция, наследование и поли-морфизм); классы и объекты; интерфейсы и реализация.

Контрольные вопросы для проверки текущих знаний студентов

Аттестационная контрольная работа №1

1. Информационная сфера и информационная среда.
2. Виды защищаемой информации.
3. Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации.
4. Виды угроз информационной безопасности объекту защиты и их характеристика.
5. Модель нарушителя информационной безопасности.
6. Модель угрозы информационной безопасности.
7. Структура сил и средств организационной защиты информации.
8. Функции, задачи и особенности службы безопасности организации.
9. Принципы организации службы безопасности организации.
10. Типовая структура службы безопасности.
11. Основные документы, регламентирующие деятельность службы безопасности объекта.
12. Участие сотрудников в организационной защите информации.
13. Взаимодействие службы безопасности объекта с правоохранительными органами.

Аттестационная контрольная работа №2

1. Обеспечение режима секретности при проведении НИОКР по секретной (конфиденциальной) тематике, при разработке и изготовлении изделий, их опытной эксплуатации и серийном производстве.
2. Требования режима секретности при работе с секретными документами.
3. Назначение и задачи секретного делопроизводства.
4. Порядок разработки, учета, хранения, размножения и уничтожения секретных (конфиденциальных) документов.
5. Понятия допуска к секретной (конфиденциальной) информации и доступа к (конфиденциальным) работам, документам и изделиям.
6. Формы допусков.
7. Служебное расследование нарушений режима секретности.

8. Организация работ по защите информации при опубликовании открытых материалов.
9. Подсистема контроля доступа и аудита.
10. Подсистема администрирования безопасности.

Аттестационная контрольная работа № 3

1. Назначение и требования внутриобъектового режима.
2. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации.
3. Требования к помещениям, в которых циркулирует защищаемая информация.
4. Понятие пропускного режима.
5. Цели и задачи пропускного режима.
6. Организация пропускного режима.
7. Атрибутные и биометрические идентификаторы людей.
8. Порядок оформления и выдачи пропусков.
9. Оценка ущерба и анализ рисков информационной безопасности.
10. Оценка затрат на организацию и проведение мероприятий по обеспечению информационной безопасности.

Перечень вопросов на экзамен

1. Информационная сфера и информационная среда.
2. Виды защищаемой информации.
3. Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации.
4. Виды угроз информационной безопасности объекту защиты и их характеристика.
5. Модель нарушителя информационной безопасности.
6. Модель угрозы информационной безопасности.
7. Структура сил и средств организационной защиты информации.
8. Функции, задачи и особенности службы безопасности организации.
9. Принципы организации службы безопасности организации.
10. Типовая структура службы безопасности.
11. Основные документы, регламентирующие деятельность службы безопасности объекта.
12. Участие сотрудников в организационной защите информации.
13. Взаимодействие службы безопасности объекта с правоохранительными органами.
14. Обеспечение режима секретности при проведении НИОКР по секретной (конфиденциальной) тематике, при разработке и изготовлении изделий, их опытной эксплуатации и серийном производстве.
15. Требования режима секретности при работе с секретными документами.
16. Назначение и задачи секретного делопроизводства.
17. Порядок разработки, учета, хранения, размножения и уничтожения секретных (конфиденциальных) документов.
18. Понятия допуска к секретной (конфиденциальной) информации и доступа к (конфиденциальным) работам, документам и изделиям.
19. Формы пропусков.
20. Служебное расследование нарушений режима секретности.
21. Организация работ по защите информации при опубликовании открытых материалов.
22. Подсистема контроля доступа и аудита.
23. Подсистема администрирования безопасности.
24. Назначение и требования внутриобъектового режима.

25. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации.
26. Требования к помещениям, в которых циркулирует защищаемая информация.
27. Понятие пропускного режима.
28. Цели и задачи пропускного режима.
29. Организация пропускного режима.
30. Атрибутные и биометрические идентификаторы людей.
31. Порядок оформления и выдачи пропусков.
32. Оценка ущерба и анализ рисков информационной безопасности.
33. Оценка затрат на организацию и проведение мероприятий по обеспечению информационной безопасности.
34. Порядок организации информационной безопасности объекта при осуществлении международного нацнотехнического и экономического сотрудничества.
35. Основные требования, предъявляемые к подготовке служебного совещания.
36. Организация обеспечения режима секретности при проведении служебного совещания.
37. Требования к помещениям для проведения совещания

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)
«Комплексное обеспечение информационной безопасности автоматизированных систем»

7.1. Рекомендуемая литература и источники информации

Зав. библиотекой _____



№	Виды занятий (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 литературы	
					в библиот	на каф
ОСНОВНАЯ						
1.	Лк. лб. срс	Безопасность и управление доступом в информационных системах. Учебное пособие	Васильков А	Москва: Форум. 2010. –368.	http://www.iprb ookshop.ru/615 58	
2.	Лк. пр. срс	Организация и технология защиты информации	Сердюк В.А	Москва: Изд.дом НИУ ВШЭ. 2011. – 328 с.	http://www.iprb ookshop.ru/292 57	
3.	Лк. пр. срс	Защита компьютерной информации. Учебное пособие	Шаньгин В.Ф	Электрон. текстовые дан. 2001г., «Кудиц-образ». 386с – Москва :	http://www.iprb ookshop.ru/244 51	
ДОПОЛНИТЕЛЬНАЯ						
4.	Лк, лб. срс	Организационная защита информации: учебное пособие для вузов Флинта	Аверченков В.И.	Интернет-университет информ. технологий. 2010 г.	http://www.iprb ookshop.ru/737 33.html	
5.	Лк, лб, срс	Защита информации в автоматизированных системах обработки данных	Герасименко в.А.	М., Энергоавтомиздат, 2016	http://www.iprb ookshop.ru/426 3215	
ИНТЕРНЕТ РЕСУРСЫ						
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.				
9.	http://fstec.ru/	http://fstec.ru/				

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.



8. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий на факультете имеется комплект технических средств обучения в составе:

- интерактивная доска;
- переносной компьютер (в конфигурации не хуже: процессор IntelCore 2 Duo, 2 Гбайта ОЗУ, 500 Гбайт НЖМД);
- проектор (разрешение не менее 1280x1024);

Для проведения лабораторных занятий имеется компьютерный класс, оборудованный компьютерами с установленным программным обеспечением, предусмотренным программой дисциплины.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем»

Рецензент от выпускающей кафедры по специальности
 подпись,  ФИО