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

РЕКОМЕНДОВАНО К УТВЕРЖДЕНИЮ	**УТВЕРЖДАЮ**
Декан, председатель совета факультета КТВТиЭ	**Проректор по учебной работе, председатель методического совета ДГТУ**
_____ **Ш. А. Юсуфов**	_____ **Н. С. Суракатов**
«18» 10 **2018 г.**	«21» 10 **2018 г.**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина Б1.В.ОД.8 Комплексное обеспечение информационной безопасности автоматизированных систем

Направление 10.03.01 – Информационная безопасность

Профиль 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 бакалавр

Форма обучения очная ; курс4; семестр 8;

Всего трудоемкость в зачетных единицах (часах) 3ЗЕТ (108 часа)

Лекции 16 (час); зачет -

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

лабораторные занятия 16 (час); самостоятельная работа 40 (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 направлению 10.03.01 – «Информационная безопасность», профилю «Безопасность автоматизированных 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 бакалавриата

Дисциплина «Комплексное обеспечение информационной безопасности автоматизированных систем» относится к обязательным дисциплинм 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:

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

способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);

способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15).

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.

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

Общая трудоемкость дисциплины составляет 3 зачетных единиц – 108 часов, в том числе: лекционных -16 часов, лабораторных - 16 часа, СРС – 40 часов, форма отчетности экзамен в 8 семестре.

4.1.Содержание дисциплины

№ п/п	Раздел дисциплины Тема лекции и вопросы	Семестр	Неделясеместра	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: «Место организационного обеспечения информационной безопасности в системе комплексной защиты информации»** Информационная сфера и информационная среда. Виды защищаемой информации.	8	1	2		2	5	Вх. Контр.
2.	**Лекция №2** **Тема: «Анализ и оценка угроз информационной безопасности информационной системы»** Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической зашитой информации. Виды угроз информационной безопасности объекту зашиты и их характеристика. Модель нарушителя информационной безопасности. Модель угрозы информационной безопасности.		2	2		2	5	
3.	**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.		3	2		2	5	

4.	**Лекция №4** **Тема: «Организация и обеспечение режима секретности»** 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.		4	2		2	5	
5.	**Лекция № 5** **Тема: «Архитектура систем защиты информации»** Подсистема контроля доступа и аудита. Подсистема администрирования безопасности.		5	2		2	5	АКР №1
6.	**Лекция № 6** **Тема: «Организация и обеспечение работ по защите информации»** 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.		6	2		2	5	
7.	**Лекции № 7** **Тема: «Методы оценки безопасности информации на объектах ее обработки»** Оценка ущерба и анализ рисков информационной безопасности. Оценка затрат на организацию и проведение мероприятий по обеспечению информационной безопасности.		7	2		2	5	

8.	**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		8	2		2	5	
	Итого по дисциплине			**16**		**16**	**40**	**Экзамен**

4.2. Содержание лабораторных занятий

№ п/п	№ лекции Из рабочей 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»	№№ 1-5	2
2	Лк №2	Тема: «Анализ и оценка угроз информационной безопасности информационной системы»	№№ 1-5	2
3	Лк №3	Тема: «Организационные источники и каналы утечки информации»	№№ 1-5	2
4	Лк № 4	Тема: «Организация и обеспечение режима секретности»	№№ 1-5	2
5	Лк № 5	Тема: «Архитектура систем защиты информации»	№№ 1-5	2
6	Лк №6	Тема: «Организация и обеспечение работ по защите информации»	№№ 1-5	2
7	Лк № 7	Тема: «Методы оценки безопасности информации на объектах ее обработки»	№№ 1-5	2
8	Лк №8	Тема: «Организация защиты информации при осуществлении международного сотрудничества»	№№ 1-5	2
Итого по дисциплине				**16**

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	Форма контроля СРС
1.	Тема: «Место организационного обеспечения информационной безопасности в системе комплексной защиты информации»	5	№№ 1-5	Опрос, реферат, статья
2.	Тема: «Анализ и оценка угроз информационной безопасности информационной системы»	5	№№ 1-5	Опрос, реферат, статья
3.	Тема: «Организационные источники и каналы утечки информации»	5	№№ 1-5	Опрос, реферат, статья
4.	Тема: «Организация и обеспечение режима секретности»	5	№№ 1-5	Опрос, реферат, статья
5.	Тема: «Архитектура систем защиты информации»	5	№№ 1-5	Опрос, реферат, статья
6.	Тема: «Организация и обеспечение работ по защите информации»	5	№№ 1-5	Опрос, реферат, статья
7.	Тема: «Методы оценки безопасности информации на объектах ее обработки»	5	№№ 1-5	Опрос, реферат, статья
8.	Тема: «Организация защиты информации при осуществлении международного сотрудничества»	5	№№ 1-5	Опрос, реферат, статья
Итого		**40**		

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки 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. Информация и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?

.

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 зашитой информации.
4. Виды угроз информационной безопасности объекту зашиты 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 допусков.
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.

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 зашитой информации.
4. Виды угроз информационной безопасности объекту зашиты 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 допусков.
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 научнотехнического 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. Информационная сфера и информационная среда.
2. Виды защищаемой информации.
3. Виды угроз информационной безопасности объекту зашиты и их характеристика.
4. Модель нарушителя информационной безопасности.
5. Модель угрозы информационной безопасности.
6. Структура сил и средств организационной защиты информации.
7. Обеспечение режима секретности при проведении НИОКР по секретной (конфиденциальной) тематике, при разработке и изготовлении изделий, их опытной эксплуатации и серийном производстве.
8. Требования режима секретности при работе с секретными документами.
9. Организация работ по защите информации при опубликовании открытых материалов.
10. Подсистема контроля доступа и аудита.
11. Подсистема администрирования безопасности.
12. Назначение и требования внутриобъектового режима.
13. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации.
14. Организация обеспечения режима секретности при проведении служебного совещания.
15. Требования к помещениям для проведения совещания

7. Учебно-методическое и информационное обеспечение дисциплины (модуля) «Комплексное обеспечение информационной безопасности автоматизированных систем»

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	
					в библ	на каф
ОСНОВНАЯ ЛИТЕРАТУРА						
1.	Лк, лб, срс	Безопасность и управление доступом в информационных системах. Учебное пособие	Васильков А	Москва: Форум. 2010. –368.	http://www.iprbookshop.ru/61558	
2.	Лк, пр, срс	Организация и технология защиты информации	Сердюк В.А	Москва: Изд.дом НИУ ВШЭ. 2011 . – 328 с.	http://www.iprbookshop.ru/29257	
3.	Лк, пр, срс	Защита компьютерной информации. Учебное пособие	Шаньгин В.Ф	Электрон. текстовые дан. 2001г., «Кудиц-образ», 386с – Москва :	http://www.iprbookshop.ru/24451	
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА						
4.	Лк, лб, срс	Организационная защита информации: учебное пособие для вузов Флинта	Аверченков В.И.	Интернет-университет информ. технологий, 2010 г.	http://www.iprbookshop.ru/73733.html	
5.	Лк, лб, срс	Защита информации в автоматизированных системах обработки данных	Герасименко в.А.	М.. Энергоавтомиздат. 2016	http://www.iprbookshop.ru/4263215	
ИНТРЕНЕТ РЕСУРСЫ						
6.	Лк, лб, срс	http://www.interface.ru - энциклопедия информационных технологий				
7.	Лк, лб, срс	http://window.edu.ru – единое окно доступа к образовательным ресурсам				
8.	Лк, лб, срс	http://www.intuit.ru – интернет-университет				
9.	Лк, лб, срс	http://www.e.lanbook.com/books "Электронно-библиотечная система				

10.	Лк, лб, срс	www.twirpx.com ресурс для студентов и преподавателей

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 направлению 10.03.01 «Информационная безопасность», профилю №Безопасность автоматизированных систем».

Рецензент от выпускающей кафедры по направлению 10.03.01 Информационная безопасность

подпись. ФИО