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

РЕКОМЕНДОВАНО
К УТВЕРЖДЕНИЮ:
Декан, председатель совета факультета Компьютерных технологий, вычислительной техники и энергетики
_____ **Ш. А. Юсуфов**
подпись ИОФ
«19» 10 **2018г.**

УТВЕРЖДАЮ:
Проректор по учебной работе, председатель методического совета ДГТУ
_____ **Н.С. Суракатов**
подпись ИОФ
«23» 10 **2018г.**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина Б1.Б.15 Основы информационной безопасности
наименование дисциплины по ООП и код по ФГОС

по направлению 10.03.01- «Информационная безопасность
шифр и полное наименование направления

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 (степень) бакалавр
бакалавр (специалист)

Форма обучения очная, курс 1 семестр (ы)1
очная, заочная, др.

Всего трудоемкость в зачетных единицах (часах) 2ЗЕТ (72 часа):
лекции 34 (час); экзамен -;
(семестр)

практические (семинарские) занятия 17 (час); зачет 1 (семестр)
(семестр)

лабораторные занятия -(час); самостоятельная работа 21 (час);

курсовой проект (работа, РГР)-(семестр)

Зав. кафедрой ИБ _____ Г.И. Качаева
подпись

Начальник УО _____ Э.В. Магомаева
подпись

1

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01- «Информационная безопасность», профиль «Безопасность автоматизированных систем»

Программа одобрена на заседании выпускающей кафедры от 15.10.18 года, протокол № 2.

Зав. выпускающей кафедрой по направлению «Информационная безопасность»

_____ Хачаева Г.И.
подпись ИОФ

ОДОБРЕНО:
Методической комиссией по
укрупненным группам специальностей и
направлению подготовки
10.00.00- «Информационная безопасность»
Председатель МК

_____ В.В. Молекин
подпись ИОФ

«15» 10 2018г.

АВТОР (Ы) ПРОГРАММЫ:

З.Р. Раджабова , к.э.н.. ст. преп. каф. ИБ
И.О.Ф. уч. степень, ученое звание, подпись

1. Цели и задачи освоения дисциплины «Основы информационной безопасности»

1.1. Цели дисциплины

- заложить терминологический фундамент
- научить правильно проводить анализ угроз информационной безопасности
- научить правильно проводить анализ угроз информационной безопасности выполнять основные этапы решения задач информационной безопасности приобрести навыки анализа угроз информационной безопасности
- рассмотреть основные общеметодологические принципы теории информационной безопасности
- изучение методов и средств обеспечения информационной безопасности
- изучение методов нарушения конфиденциальности, целостности и доступности информации

1.2.Задачи дисциплины

- ознакомление студентов с терминологией информационной безопасности
- развитие мышления студентов
- изучение методов и средств обеспечения информационной безопасности
- обучение определению причин, видов, каналов утечки и искажения информации

2. Место дисциплины «Основы информационной безопасности»в структуре ООП бакалавриата

Дисциплина «Основы информационной безопасности» относится к базовой части ФГОС ВО. Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: информатика, математика.

Последующими дисциплинами являются: Безопасность операционных систем.

Общая трудоемкость дисциплины составляет 2 зачетные единицы.

Рекомендуемая форма итогового контроля- экзамен.

3.Процесс изучения дисциплины «Основы информационной безопасности» направлен на формирование следующих компетенций

Процесс изучения дисциплины направлен на формирование следующих концепций:

ОК-4 - способностью использовать основы правовых знаний в различных сферах деятельности;

ОК-5 - способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

ОПК-4 - способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5 - способностью использовать нормативные правовые акты в профессиональной деятельности;

Знать:

- сущность и понятие информационной безопасности и характеристику ее составляющих;
- место и роль информационной безопасности в системе национальной безопасности Российской Федерации,
- основы государственной информационной политики,
- стратегию развития информационного общества в России;
- источники и классификацию угроз информационной безопасности;
- основные средства и способы обеспечения информационной безопасности,
- принципы построения систем защиты информации.

Уметь:

- классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности;
- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.

Владеть:

- профессиональной терминологией в области информационной безопасности

4. Структура и содержание дисциплины «Основы информационной безопасности»

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	
1	**Лекция № 1** **Тема: «Понятие составляющие и система формирования режима информационной безопасности»** 1. Определение понятия "информационная безопасность" 2. Доступность ,целостность и конфиденциальность информации	1	1	2	2	-	-	Вх. контр. работа
2	**Лекция №2** **Тема: «Понятие составляющие и система формирования режима информационной безопасности»** 1. Задачи информационной безопасности общества. 2. Уровни формирования режима информационной безопасности		2	2		-	2	Контрольная работа № 1
3	**Лекции №3** **Тема: «Нормативно-правовые основы информационной безопасности в РФ».** 1. Правовые основы информационной безопасности общества. 2. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. 3. Ответственность за нарушения в сфере информационной безопасности.		3	2	2	-	2	
4	**Лекция №4** **Тема: «Стандарты информационной безопасности».** 1. Стандарты информационной безопасности: "Общие критерии". 2. Стандарты информационной безопасности распределенных систем		4	2	-	-	-	
5	**Лекция №5** **«Стандарты информационной безопасности».** 1 Стандарты информационной безопасности в РФ.		5	2	2	-	2	
6	**Лекция №6** **Тема: «Административный уровень обеспечения информационной безопасности»** 1. Цели, задачи и содержание административного уровня. 2. Разработка политики информационной безопасности.		6	2	-	-	-	
7	**Лекции №7** **Тема: «Классификация угроз "информационной безопасности"»** 1. Классы угроз информационной безопасности. 2.Каналы несанкционированного доступа к информации		7	2	2	-	2	Контрольная работа № 2
8	**Лекция №8** **Тема: «Вирусы как угроза информационной безопасности».** 1.Компьютерные вирусы и информационная безопасность. 2.Характерные черты компьютерных вирусов.		8	2		-	2	
9	**Лекция №9** **Тема: «Классификация компьютерных вирусов»** 1. Классификация компьютерных вирусов по среде обитания. 2. Классификация компьютерных вирусов по особенностям алгоритма работы. 3. Классификация компьютерных вирусов по деструктивные возможностям		9	2	2	-	2	
10	**Лекция № 10** **Тема: «Характеристика "вирусоподобных" программ. Антивирусные программы»** 1. Виды "вирусоподобных" программ. 2. Характеристика "вирусоподобных" программ Государственное экономическое регулирование. Объекты и цели ГРЭ 3. Утилиты скрытого администрирования		10	2	-	-	2	

11	**Лекция № 11** **Тема: «Характеристика "вирусоподобных" программ. Антивирусные программы»** 1."Intended"-вирусы. 2. Особенности работы антивирусных программ. Классификация антивирусных программ 3. Факторы, определяющие качество антивирусных программ		11	2	2	-	-	
12	**Лекция № 12** **Тема: «Профилактика компьютерных вирусов. Обнаружение неизвестного вируса».** 1. Характеристика путей проникновения вирусов в компьютеры. 2. Правила защиты от компьютерных вирусов 3. Обнаружение загрузочного и резидентного вируса, макровируса 4. Общий алгоритм обнаружения вируса	1	12	2	-	-	2	Контрольная работа №3
13	**Лекция № 13** **Тема: «Информационная безопасность вычислительных сетей».** 1. Особенности обеспечения информационной безопасности в компьютерных сетях 2. Сетевые модели передачи данных. 3. Модель взаимодействия открытых систем OSI/ISO. 4. Адресация в глобальных сетях.		13	2	2		2	
14	**Лекция № 14** **Тема: «Удаленные угрозы в вычислительных сетях»** 1. Классификация удаленных угроз в вычислительных сетях 2. Типовые удаленные атаки и их характеристика		14	2	-	-	-	
15	**Лекция № 15** **Тема: «Удаленные угрозы в вычислительных сетях»** 1. Причины успешной реализации удаленных угроз в вычислительных сетях 2. Принципы защиты распределенных вычислительных сетей		15	2	2	-	2	
16	**Лекция № 16** **Тема: «Механизмы обеспечения "информационной безопасности"»** 1. Идентификация и аутентификация 2. Криптография и шифрование 3. Методы разграничение доступа		16	2	-	-	-	
17	**Лекция № 17** **Тема: «Механизмы обеспечения "информационной безопасности"»** 1. Регистрация и аудит 2. Межсетевое экранирование 3. Технология виртуальных частных сетей (VPN)		17	2	1		1	
	Итого		**17**	**34**	**17**		**21**	**Зачет**

1.2. Содержание практических занятий

№ п/п	№ лекции из рабочей программы	Наименование практического, семинарского занятия	Количество часов	Рекомендуемая литература и методические разработки (№ источника из списка литературы)
1	**2**	**3**	**4**	**5**
1	1,	«Ответственность за нарушения в сфере информационной безопасности»	2	1-11
2	2,3	«Стандарты информационной безопасности РФ»	2	1,2,5,10,11
3	4,5	«Разработка политики информационной безопасности»	2	2,3,5,9,10
4	6,7	«Каналы несанкционированного доступа к информации	2	1,3,6,7,10,11
5	8,9	«Характерные черты компьютерных вирусов»	2	1,3,6,7,10,11
6	10,11	«Факторы, определяющие качество антивирусных программ «	2	2,10
7	12,13	«Адресация в глобальных сетях»	2	1,3,4,7,8.10,11
8	14,15	«Принципы защиты распределенных вычислительных сетей»	2	2,4,6,8,10,11
9	16,17	«Технология виртуальных частных сетей (VPN)»	1	1,2,5,10,11
Итого			**17**	

4.3 Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Количество часов из содержания дисциплины	Рекомендуемая литература и источники информации	Формы контроля СРС
1	2	3	4	5
1	«Понятие составляющие исистема формирования режима информационной безопасности»	2	1,2,5,10,11	Доклад
2	«Нормативно-правовые основы информационной безопасности в РФ»	2	2,3,5,9,10	Реферат
3	«Стандарты информационной безопасности»	2	1,3,6,7,10,11	Доклад
4	«Административный уровень обеспечения информационной безопасности»	2	2,10	Доклад
5	«Классификация угроз "информационной безопасности"»	2	5,6,4,10	Доклад
6	«Вирусы как угроза информационной безопасности».	2	1,3,4,7,8.10,11	Реферат
7	«Классификация компьютерных вирусов»	2	2,4,6,8,10,11	Доклад
8	«Характеристика "вирусоподобных" программ. Антивирусные программы»	2	2,3,5,8,10	Реферат
9	«Профилактика компьютерных вирусов. Обнаружение неизвестного вируса»	2	1,5,8,10	Реферат
10	«Информационная безопасность вычислительных сетей»	1	1,2,5,10,11	Доклад
11	«Удаленные угрозы в вычислительных сетях»	1	2,3,5,9,10	Реферат
12	«Механизмы обеспечения "информационной безопасности"»	1	2,10,	Доклад
	Итого	**21**		

5.Образовательные технологии

В рамках курса «Основы информационной безопасности» уделяется особое внимание установлению межпредметных связей, демонстрации возможности применения полученных знаний в практической деятельности.

В лекционных занятиях используются следующие инновационные методы:

- **групповая форма обучения** - форма обучения, позволяющая обучающимся эффективно взаимодействовать в микрогруппах при формировании и закреплении знаний;
- **компетентностный подход к оценке знаний** - это подход, акцентирующий внимание на результатах образования, причем в качестве результата рассматривается не сумма усвоенной информации, а способность человека действовать в различных проблемных ситуациях;
- **личностно-ориентированное обучение**- это такое обучение, где во где во главу угла ставится личность обучаемого, ее самобытность, самоценность, субъективный опыт каждого сначала раскрывается, а затем согласовывается с содержанием образования;
- **междисциплинарный подход**- подход к обучению, позволяющий научить студентов самостоятельно «добывать» знания из разных областей, группировать их и концентрировать в контексте конкретной решаемой задачи;
- **развивающее обучение**- ориентация учебного процесса на потенциальные возможности человека и их реализацию. В концепции развивающего обучения учащийся рассматривается не как объект обучающих воздействий учителя, а как самоизменяющийся субъект учения.

В процессе выполнения практических занятий используются следующие методы:

- **исследовательский метод обучения –** метод обучения, обеспечивающий возможность организации поисковой деятельности обучаемых по решению новых для них проблем,

процессе которой осуществляется овладение обучаемыми методами научными познания и развитие творческой деятельности;

- **метод рейтинга -** определение оценки деятельности личности или события. В последние годы начинает использоваться как метод контроля и оценки в учебно-воспитательном процессе;
- **проблемно-ориентированный подход-** подход к обучению позволяющий сфокусировать внимание студентов на анализе и разрешении, какой либо конкретной проблемной ситуации, что становится отправной точкой в процессе обучения.

Удельный вес занятий, проводимых в интерактивной форме, составляют не менее 20% аудиторных занятий (25 ч.).

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

6.1.Вопросы для входной контрольной работы

1.Органы, обеспечивающие национальную безопасность Российской Федерации, цели, задачи.
2. Национальные интересы Российской Федерации в информационной сфере.
3. Приоритетные направления в области защиты информации в Российской Федерации.
4. Тенденции развития информационной политики государств и ведомств. Информационная война, проблемы.
5. Правовое обеспечение защиты информации.
6. Информация с ограниченным доступом, государственная тайна, конфиденциальность, коммерческая тайна, персональные данные.
7.

6.2.Контрольные работы по проверке текущих знаний студентов

Контрольная работа №1

1. Определение понятия "информационная безопасность"
2. Доступность , целостность и конфиденциальность информации
3. Задачи информационной безопасности общества.
4. Уровни формирования режима информационной безопасности
5. Правовые основы информационной безопасности общества
6. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации
7. Ответственность за нарушения в сфере информационной безопасности
8. Стандарты информационной безопасности: "Общие критерии"
9. Стандарты информационной безопасности распределенных систем
10. Стандарты информационной безопасности в РФ.
11. Цели, задачи и содержание административного уровня.
12. Разработка политики информационной безопасности.

Контрольная работа №2

1. Классы угроз информационной безопасности
2. Каналы несанкционированного доступа к информации
3. Компьютерные вирусы и информационная безопасность.
4. Характерные черты компьютерных вирусов

5. Классификация компьютерных вирусов по среде обитания.
6. Классификация компьютерных вирусов по особенностям алгоритма работы.
7. Классификация компьютерных вирусов по деструктивные возможностям
8. Виды "вирусоподобных" программ.
9. Характеристика "вирусоподобных" программ Государственное экономическое регулирование. Объекты и цели ГРЭ
10. Утилиты скрытого администрирования
11. "Intended"-вирусы.
12. Особенности работы антивирусных программ. Классификация антивирусных программ
13. Факторы, определяющие качество антивирусных программ

Контрольная работа №3

1. Характеристика путей проникновения вирусов в компьютеры
2. Правила защиты от компьютерных вирусов
3. Обнаружение загрузочного и резидентного вируса макровируса
4. Общий алгоритм обнаружения вируса
5. Сетевые модели передачи данных.
6. Модель взаимодействия открытых систем OSI/ISO
7. Особенности обеспечения информационной безопасности в компьютерных сетях
8. Адресация в глобальных сетях.
9. Принципы защиты распределенных вычислительных сетей
10. Классификация удаленных угроз в вычислительных сетях
11. Типовые удаленные атаки и их характеристика
12. Причины успешной реализации удаленных угроз в вычислительных сетях
13. Технология виртуальных частных сетей (VPN)
14. Идентификация и аутентификация
15. Криптография и шифрование
16. Методы разграничение доступа
17. Регистрация и аудит
18. Межсетевое экранирование

6.3.Вопросы к зачету по дисциплине «Основы информационной безопасности»

1. Определение понятия "информационная безопасность"
2. Доступность , целостность и конфиденциальность информации
3. Задачи информационной безопасности общества.
4. Правовые основы информационной безопасности общества
5. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации
6. Ответственность за нарушения в сфере информационной безопасности
7. Стандарты информационной безопасности: "Общие критерии"
8. Стандарты информационной безопасности распределенных систем
9. Стандарты информационной безопасности в РФ.
10. Цели, задачи и содержание административного уровня.
11. Разработка политики информационной безопасности.
12. Классы угроз информационной безопасности
13. Каналы несанкционированного доступа к информации
14. Компьютерные вирусы и информационная безопасность.
15. Характерные черты компьютерных вирусов
16. Классификация компьютерных вирусов по среде обитания.

17. Классификация компьютерных вирусов по особенностям алгоритма работы.
18. Классификация компьютерных вирусов по деструктивные возможностям
19. Виды "вирусоподобных" программ.
20. Характеристика "вирусоподобных" программ Государственное экономическое регулирование. Объекты и цели ГРЭ
21. Утилиты скрытого администрирования
22. "Intended"-вирусы.
23. Особенности работы антивирусных программ. Классификация антивирусных программ
24. Факторы, определяющие качество антивирусных программ
25. Характеристика путей проникновения вирусов в компьютеры
26. Правила защиты от компьютерных вирусов
27. Обнаружение загрузочногоирезидентного вируса,макровируса
28. Общий алгоритм обнаружения вируса
29. Сетевые модели передачи данных.
30. Модель взаимодействия открытых систем OSI/ISO
31. Особенности обеспечения информационной безопасности в компьютерных сетях
32. Адресация в глобальных сетях.
33. Принципы защиты распределенных вычислительных сетей
34. Классификация удаленных угроз в вычислительных сетях
35. Типовые удаленные атаки и их характеристика
36. Причины успешной реализации удаленных угроз в вычислительных сетях
37. Технология виртуальных частных сетей (VPN)
38. Идентификация и аутентификация
39. Криптография и шифрование
40. Методы разграничение доступа
41. Регистрация и аудит
42. Межсетевое экранирование

6.4.Вопросы для проверки остаточных знаний по дисциплине «Основы информационной безопасности»

1. Понятие составляющие и система формирования режима информационной безопасности
2. Нормативно-правовые основы информационной безопасности в РФ
3. Стандарты информационной безопасности
4. Административный уровень обеспечения информационной безопасности.
5. Классификация угроз "информационной безопасности"
6. Классификация компьютерных вирусов
7. Антивирусные программы

7. Учебно-методическое и информационное обеспечение дисциплины

Рекомендуемая литература и источники информации (основная и дополнительная) по дисциплине «Основы информационной безопасности»

№п\п	Видызаня тий	Комплект необходимой учебной литературы по дисциплине	Автор	Издат. и год изд.	Количество пособий, учебников и прочей литературы	
					В библ.	На каф.
Основная литература						
1.	ЛЗ, ПЗ, СРС	Основы информационной безопасности	Галатенко В. А.	М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2013.	3	1
2.	ЛЗ, ПЗ, СРС	Основы информационной безопасности: учеб. пособие для вузов	Белов Е.Б. [и др.].	М. : Горячая линия-Телеком, 2006	20	1
3.	ЛЗ, ПЗ, СРС	Основы информационной безопасности [Электронный ресурс]	Галатенко, В. А.	М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — 978-5-94774-821-5.	http://www.iprbookshop.ru/52209.html	
4.	ЛЗ, ПЗ, СРС	Основы информационной безопасности	С.П. Расторгуев.	М. : Академия, 2007. - 188 с. - (Высшее профессиональное образование).	16	1
5	ЛЗ, ПЗ, СРС	Основы информационной безопасности [Электронный ресурс]	Сычев, Ю. Н.	М.: Евразийский открытый институт, 2010. — 328 с. — 978-5-374-00381-9.	http://www.iprbookshop.ru/10746.html	
Дополнительная литература						
6.	ЛЗ, ПЗ, СРС	Основы информационной безопасности при работе на компьютере [Электронный ресурс]	Фаронов, А. Е.	М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. — 2227-8397.	http://www.iprbookshop.ru/52160.html	
7.	ЛЗ, ПЗ, СРС	Основы информационной безопасности [Электронный ресурс]	Голиков, А. М.	Томск: Томский государственный университет систем управления и радиоэлектроники, 2007. — 288 с. — 978-5-868889-467-1	http://www.iprbookshop.ru/13957.html	
8.		Основы информационной безопасности : курс лекций : учеб. пособие /.- Изд. 3-е. -	В.А. Галатенко; под ред. В.Б. Бетелина	М.: Интернет-Университет Информационных технологий, 2006. - 208 с. - (Основы информационных технологий)	5	1
Интернет - источники						
9.	ЛЗ, ПЗ, СРС	http://www.edu.ru - веб-сайт системы федеральных образовательных порталов				
10.	ЛЗ, ПЗ, СРС	http://www.sec.ru – каталог организаций в сфере информационной безопасности				
11.	ЛЗ, ПЗ, СРС	базы данных, информационно-справочные и поисковые системы: правовые справочно-поисковые системы («Гарант», «Консультант Плюс»), www.fstec.ru;www.gost.ru/wps/portal/tk362.				

12

8.Материально-техническое обеспечение дисциплины

МТО включает в себя:

- библиотечный фонд (учебная, учебно-методическая, справочная экономическая литература, экономическая научная и деловая периодика);
- компьютеризированные рабочие места для обучаемых с доступом в сеть интернет;
- аудитории, оборудованные проекционной техникой.

На технологическом факультете имеется аудитория, оборудованная интерактивной доской, проектором, что позволяет читать лекции в формате презентаций, разработанных с помощью пакета прикладных программ MSPowerPoint, использовать наглядные, иллюстрированные материалы, обширную информацию в табличной и графической форме, а также электронные ресурсы сети Интернет.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01- «Информационная безопасность», профиль «Безопасность автоматизированных систем»

Рецензент от выпускающей кафедры (работодателя) по направлению 10.03.01- «Информационная безопасность», профиль «Безопасность автоматизированных систем»

А.Г. Мустафаев, доцент кафедры

Подпись ИОФ, должность