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
«17» 10 2018г.

УТВЕРЖДАЮ
Проректор по учебной работе,
председатель методического
совета ДГТУ
Н.С. Суракатов
«22» 10 2018г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина С1.В.ОД.7 Теоретические основы компьютерной безопасности
наименование дисциплины по ООП и код по ФГОС

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, курс 3 семестр (ы) 6
очная, заочная, др

Всего трудоемкость в зачетных единицах (часах) 4 ЗЕТ (144Ч):

лекции 34 (час); экзамен - ;
(семестр)

практические (семинарские) занятия - (час); зачет 6

лабораторные занятия 17 (час); самостоятельная работа 93 (час);

курсовой проект (работа, РГР) -

Зав. кафедрой ИБ Г.И. Качаева

Начальник УО Э.В. Магомаева

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

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

Зав. выпускающей кафедрой по специализации «Безопасность открытых информационных систем»

Г.И. Попова

подпись ИОФ

ОДОБРЕНО:

Методической комиссией по укрупненным группам специальностей и направлению подготовки 10.00.00- «Информационная безопасность»

Председатель МК

Мишкин В.Б

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 «Теоретические основы компьютерной безопасности»

1.1. Цели дисциплины

Дисциплина «Теоретические основы компьютерной безопасности» изучает вопросы, связанные с приобретением необходимых знаний, умений и навыков в области современных информационных технологий, применяемых для обеспечения компьютерной безопасности.

Целью изучения дисциплины является обучение студентов обучение студентов комплексному подходу к обеспечению информационной безопасности; формирование у них представлений об использовании специального математического аппарата для анализа защищенности автоматизированных систем.

1.2.Задачи дисциплины

–получить представление об основных угрозах информационной безопасности и методах противодействия данным угрозам;

–изучить основные формальные математические модели, используемые для анализа защищенности автоматизированных систем;

–изучить методологию проектирования и построения защищенных автоматизированных систем.

2. Место дисциплины «Теоретические основы компьютерной безопасности» в структуре ООП специалитета

Дисциплина «Теоретические основы компьютерной безопасности» (С1.В.ОД.7) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность операционных систем, Безопасность сетей ЭВМ, Безопасность электронного документооборота, Дискретная математика, Основы информационной безопасности.

Основными видами занятий являются лекции и лабораторные занятия. Для освоения дисциплины наряду с проработкой лекционного материала необходимо проведение самостоятельной работы.

Основными видами текущего контроля знаний являются контрольные и лабораторные работы по каждой теме.

Основным видом рубежного контроля знаний является зачет.

3. Процесс изучения дисциплины «Теоретические основы компьютерной безопасности» направлен на формирование следующих компетенций.

В результате освоения дисциплины обучающийся должен обладать

Профессиональными компетенциями (ПК):

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

В результате изучения дисциплины студент должен:

Знать:

- методологические и технологические основы комплексного обеспечения безопасности АС;
- угрозы и методы нарушения безопасности АС;
- формальные модели, лежащие в основе систем защиты АС;
- стандарты по оценке защищенных систем и их теоретические основы;
- методы и средства реализации защищенных АС;

– средства и методы верификации и анализа надежности защищенных АС.

Уметь:

– проводить анализ АС с точки зрения обеспечения компьютерной безопасности;
– разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы;
– применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС;
– реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС.

Владеть:

– работой с АС распределенных вычислений и обработки информации;
– управлением процессами функционирования систем защиты;
– навыками работы с документацией АС;
– использованием критериев оценки защищенности АС;
– навыками построения формальных моделей систем защиты информации АС.

4. Структура и содержание дисциплины «Теоретические основы компьютерной безопасности»

Общая трудоемкость дисциплины составляет 4 зачетные единицы – 144 часа, в том числе: лекционных -34 часа, лабораторных - 17 часа, СРС – 93 часов, форма отчетности зачет в 6 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	ЛБ	СР	
1.	**Лекция № 1** **Тема 1: « Основные положения теории защиты информации»** Субъектно-объектное представление автоматизированной системы.	4	1	2		1	6	Вх. контр. работа
2.	**Лекция № 2** **Тема 1: « Основные положения теории защиты информации»** Субъектно-объектное представление автоматизированной системы.		2	2		1	6	
3.	**Лекция № 3** **Тема 1: « Основные положения теории защиты информации»** Понятие доступа. Информационная безопасность автоматизированных систем.		3	2		1	4	
4.	**Лекция № 4** **Тема2: «Математическое моделирование в проектировании защищённых телекоммуникационных систем»** Математические модели в информационной безопасности.		4	2		1	6	
5.	**Лекция № 5** **Тема2: «Математическое моделирование в проектировании защищённых телекоммуникационных систем»** Применение моделей при проектировании систем безопасности.		5	2		1	6	Аттестационная контрольная работа №1
6.	**Лекции № 6** **Тема 3: « Классификация угроз безопасности информации в Телекоммуникационных системах и их элементах».** 1. Угрозы конфиденциальности, целостности и		6	2		1	6	

	доступности информации.						
7.	**Лекции № 7** **Тема 3: « Классификация угроз безопасности информации в Телекоммуникационных системах и их элементах».** Угроза раскрытия параметров автоматизированной системы.	7	2		1	4	
8.	**Лекции № 8** **Тема 3: « Классификация угроз безопасности информации в Телекоммуникационных системах и их элементах».** Классификационные признаки угроз безопасности информации.	8	2		1	4	
9.	**Лекция № 9** **Тема 4: «Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем».** Матрица доступов.	9	2		1	6	
10.	**Лекция № 10** **Тема 4: «Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем».** Классическая модель Take-Grant.	10	2		1	4	Аттестационная контрольная работа №2
11.	**Лекция № 11** **Тема 4: «Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем».** Расширенная модель Take-Grant.	11	2		1	4	
12.	**Лекция № 12** **Тема 5: « Мандатное разграничение доступа для обеспечения безопасности телекоммуникационных систем».** Модель Белла-Ла Падула. Модель Биба.	12	2		1	6	
13.	**Лекция № 13** **Тема 5: « Мандатное разграничение доступа для обеспечения безопасности телекоммуникационных систем».** Модель систем военных сообщений .	13	2		1	6	
14.	**Лекция № 14** **Тема6: «Ролевое разграничение доступа для обеспечения безопасности телекоммуникационных систем».** Понятие роли.	14	2		1	6	
15.	**Лекция № 15** **Тема6: «Ролевое разграничение доступа для обеспечения безопасности телекоммуникационных систем».** Модель ролевого разграничения доступа.	15	2		1	6	Аттестационная контрольная работа №3
16.	**Лекции № 16** **Тема7 : «Изолированная программная среда в**	16	2		1	6	

	проектировании защищённых телекоммуникационных систем и их элементов» Монитор безопасности объектов.							
17.	**Лекции № 17 Тема7 : «Изолированная программная среда в проектировании защищённых телекоммуникационных систем и их элементов»** Монитор безопасности. Изолированная программная среда.		17	2		1	6	
Итого				**34**	**-**	**17**	**93**	**Экзамен (1зет=36 часов)**

4.2 Содержание лабораторных занятий

№ п/п	**№ лекции из рабочей программы**	**Наименование лабораторного занятия**	**Количество часов**	**Рекомендуемая литература и методические разработки (№ источника из списка литературы)**
1	**2**	**3**	**4**	**5**
1	1-3	Субъектно-объектное представление автоматизированной системы	2	№1-№11
2	4 -5	Функциональные модели автоматизированных систем	1	№1-№11
3	4 -5	Математические модели автоматизированных систем	1	№1-№11
4	6-8	Противодействие угрозам конфиденциальности, целостности и доступности информации в автоматизированных системах	4	№1-№11
5	9-11	Работа с матрицей доступов	1	№1-№11
6	9-11	Модель Take-Grant	1	№1-№11
7	12-13	Мандатное разграничение прав доступа пользователей	1	№1-№11
8	12-13	Модель Белла-ЛаПадула	1	№1-№11
9	14-15	Ролевое разграничение прав доступа пользователей	2	№1-№11
10	16-17	Построение изолированной программной среды	3	№1-№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.	Основные положения теории защиты информации	6	№1-№11	Доклад
2.	Основные положения теории защиты информации	6	№1-№11	Реферат
3.	Основные положения теории защиты информации	4	№1-№11	Доклад
4.	Математическое моделирование в проектировании защищённых телекоммуникационных систем	6	№1-№11	Доклад
5.	Математическое моделирование в проектировании защищённых телекоммуникационных систем	6	№1-№11	Доклад
6.	Классификация угроз безопасности информации в	6	№1-№11	Реферат
7.	Телекоммуникационных системах и их элементах .	4	№1-№11	Доклад
8.	Классификация угроз безопасности информации в Телекоммуникационных системах и их элементах	4	№1-№11	Доклад
9.	Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем	6	№1-№11	Реферат
10.	Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем	4	№1-№11	Доклад
11.	Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем	4	№1-№11	Доклад
12.	Мандатное разграничение доступа для обеспечения безопасности телекоммуникационных систем	6	№1-№11	Реферат
13.	Мандатное разграничение доступа для обеспечения безопасности телекоммуникационных систем	6	№1-№11	Доклад
14.	Ролевое разграничение доступа для обеспечения безопасности телекоммуникационных систем	6	№1-№11	Доклад
15.	Ролевое разграничение доступа для обеспечения безопасности телекоммуникационных систем	6	№1-№11	Доклад
16.	Изолированная программная среда в проектировании защищённых	6	№1-№11	Реферат

	телекоммуникационных систем и их элементов			
17.	Изолированная программная среда в проектировании защищённых телекоммуникационных систем и их элементов	6	№1-№11	Доклад
	Итого	**93**		

5.Образовательные технологии

В рамках курса «Теоретические основы компьютерной 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.

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. Определение понятия "информационная безопасность"
2. Доступность, целостность и конфиденциальность информации
3. Задачи информационной безопасности общества.
4. Правовые основы информационной безопасности общества
5. Стандарты информационной безопасности: "Общие критерии"
6. Стандарты информационной безопасности распределенных систем
7. Стандарты информационной безопасности в РФ.
8. Каналы несанкционированного доступа к информации
9. Компьютерные вирусы и информационная безопасность.
10. Виды "вирусоподобных" программ.
11. Сетевые модели передачи данных.
12. Модель взаимодействия открытых систем OSI/ISO
13. Особенности обеспечения информационной безопасности в компьютерных сетях
14. Адресация в глобальных сетях.
15. Принципы защиты распределенных вычислительных сетей
16. Идентификация и аутентификация
17. Криптография и шифрование
18. Методы разграничение доступа
19. Регистрация и аудит
20. Межсетевое экранирование

6.2 Контрольные работы по проверке текущих знаний студентов

Аттестационная контрольная работа №1

1. Субъектно-объектное представление автоматизированной системы.
2. Понятие доступа.
3. Информационная безопасность автоматизированных систем.
4. Математические модели в информационной безопасности.
5. Применение моделей при проектировании систем безопасности

Аттестационная контрольная работа №2

1. Угрозы конфиденциальности, целостности и доступности информации.
2. Угроза раскрытия параметров автоматизированной системы.
3. Классификационные признаки угроз безопасности информации.
4. Матрица доступов.
5. Классическая модель Take-Grant.
6. Расширенная модель Take-Grant.

Аттестационная контрольная работа №3

1. Понятие роли.
2. Модель ролевого разграничения доступа.
3. Монитор безопасности объектов.
4. Монитор безопасности.
5. Изолированная программная среда.

6.3.Вопросы к зачету по дисциплине «Теоретические основы компьютерной безопасности»

1. Что является важнейшими особенностями информации?
2. Что входит в автоматизированные системы обработки информации?
3. Дайте определение информационной безопасности автоматизированной системы.
4. Дайте определение субъекта доступа.
5. Сформулируйте основную теорему безопасности информации в АС.
6. На каком уровне иерархии модели OSI/ISO нельзя использовать модели безопасности информации?
7. На основе чего строится ценность информации в аддитивной модели?
8. Как определяется ценность информации в модель анализа риска 20. Профилактика компьютерных вирусов.
9. На чем основывается порядковая шкала ценностей?
10. В каких случаях применяется модель решетки ценностей?
11. MLS-решетка.
12. Дайте определение конфиденциальности информации.
13. Дайте определение целостности информации.
14. Дайте определение доступности информации.
15. На какие уровни разделяется доступ к информации применительно к автоматизированным системам?
16. Перечислите основные принципы обеспечения информационной безопасности в АС.
17. Чем, согласно основным принципам, должна обеспечиваться информационная безопасность в АС?
18. Чем, согласно основным принципам, является оценка эффективности обеспечения информационной безопасности в АС?
19. Приведите примеры несанкционированного копирования носителей информации.
20. Приведите примеры не информационных каналов утечки информации.
21. Какого доступа к данным машинных носителей информации не существует?
22. Дайте определение идентификации и аутентификации.
23. На чем основаны парольные системы защиты?
24. Приведите примеры угроз нарушения конфиденциальности.
25. Приведите примеры угроз нарушения целостности.
26. Приведите примеры угроз отказа служб.
27. Зачем необходим принцип системности.
28. Для чего в системе защиты информации используется принцип комплексности?
29. Приведите пример идентификации.
30. Приведите пример аутентификации.
31. Как называют процедуру аутентификации, если в ней (помимо основных сторон) участвует сервер аутентификации (арбитр)?
32. С помощью какого вредоносного программного обеспечения может быть создана атака на систему аутентификации?
33. Дайте определение пароля пользователя.
34. Каких атак на пароли не существует?
35. Перечислите компоненты парольной системы защиты.
36. Какие элементы затрудняют появление угроз парольным системам?
37. Какова зависимость между мощностью алфавита паролей и скоростью перебора паролей?
38. Какова зависимость параметров парольной системы защиты от длины пароля?
39. Как расшифровывается аббревиатура СКЗИ?
40. Какие существуют системы шифрования?

41. Для чего необходимо шифрование?
42. Для чего необходима электронно-цифровая подпись?
43. Дайте определение стеганографии.
44. Приведите примеры стеганографических приемов защиты информации.
45. В чем заключается сертификация средств СКЗИ?
46. Какие стандарты защиты информации на данный момент действуют в Российской Федерации?
47. В чем заключается требование корректности транзакций?
48. В чем заключается принцип минимизации привилегий?
49. Что подразумевает разграничение функциональных обязанностей в АС?
50. Для чего необходим аудит произошедших событий в АС?
51. В каких случаях требуется обеспечение непрерывной работы защитных механизмов АС?
52. В чем заключается требование простоты использования защитных механизмов?
53. Каково назначение модели Кларка – Вилсона?
54. Перечислите правила модели Кларка-Вилсона.
55. Для чего используются барьерные адреса? Варианты назначения барьерных адресов.
56. Позволяет ли использование сегментов оперативной памяти защитить код программ друг от друга?
57. Позволяет ли использование сегментов оперативной памяти обеспечить доступ нескольких программ к одному участку оперативной памяти?
58. Чем обеспечивается отказоустойчивость программного обеспечения (ПО) АС?
59. Дайте определение политики безопасности.
60. Между какими элементами системы существуют потоки информации?
61. При каком условии возможно порождение субъекта?
62. Какое действие называется доступом субъекта S к объекту O?
63. Какой из специальных субъектов системы является механизмом реализации заданной политики безопасности системы?
64. Перечислите типы политик безопасности.
65. Какой тип политик безопасности может противостоять атакам типа «Троянский конь» ?
66. Какими свойствами определяется дискреционное управление доступом?
67. Какими свойствами определяется мандатное управление доступом?
68. Как определяется корректность субъектов друг относительно друга?
69. Каково назначение Монитора безопасности субъектов и Монитора безопасности объектов?
70. Какие специальные субъекты обязательно входят в состав Изолированной программной среды?
71. Для чего используются модели политик безопасности?
72. Какие из известных Вам моделей политик безопасности используются для представления систем, реализующих дискреционное управление доступом?
73. Какие из известных Вам моделей политик безопасности используются для представления систем, реализующих мандатное управление доступом?
74. В чем состоит основная задача дискреционных политик безопасности?
75. В чем состоит основная задача мандатных политик безопасности?
76. Какие операции преобразования матрицы доступов используются в модели HRU?
77. Возможна ли проверка безопасности произвольной системы, представленной моделью матрицы доступов HRU?
78. Какая система в модели HRU называется монооперационной?
79. Что является основой политики MLS?

80. При каком условии согласно политике MLS разрешен доступ субъекта S к объекту O?
81. При помощи чего в модели Take-Grant описывается функционирование системы?
82. Какие команды преобразования графа доступов используются в модели Take-Grant?
83. В каком случае возможно похищение прав доступа согласно модели Take-Grant?
84. Каково назначение расширенной модели Take-Grant?
85. Можно ли применять правила де-юре к мнимым дугам в расширенной модели Take-Grant?
86. С помощью каких свойств определяется безопасность системы в модели Белла-Лападула?
87. Что является основной задачей стандартов информационной безопасности?
88. Укажите назначение профиля защиты.
89. Перечислите виды оценок согласно РД «Общие критерии».

Тестовые задания

1. Какова роль монитора безопасности объектов и монитора безопасности субъектов в субъектно-объектной модели при проектировании защищённых автоматизированных систем?

a) Разрешает порождение субъектов только для фиксированного подмножества пар активизирующих субъектов и порождающих объектов;
b) Разрешает поток, принадлежащий только множеству легального доступа;
c) Активизируется при порождении субъектов;
d) Сокращает множество возможных объектов до некоторого множества фиксированной мощности.

2. К общим принципам создания и эксплуатации защищенных автоматизированных систем не относится …

a) Принцип системности;
b)Принцип непрерывности;
c) Принцип разумной достаточности;
d) Принцип минимизации стоимости.

3. К методам и механизмам обеспечения информационной безопасности безопасности автоматизированных систем непосредственного действия относится …

a) Управление сетевыми соединениями;
b) Разграничение доступа к данным;
c) Нормативно-организационная регламентация;
d) Управление сеансами.

4. К задачам аудита информационной безопасности не относится…

a) Прогноз рисков;
b) Оценка текущего уровня безопасности;
c) Разработка рекомендаций по повышению уровня безопасности;
d) Разработка новых средств защиты информации.

5. Мощность пространства паролей …

a) Прямо пропорциональна вероятности подбора пароля;
b) Зависит от срока действия пароля;
c) Прямо пропорциональна мощности алфавита пароля;
d) Влияет на длину пароля.

6. Использование защитных механизмов различной и наиболее целесообразной в конкретных условиях природы на всех этапах функционирования автоматизированной системы и ее элементов обеспечивается …

a) Принципом комплексности;
b) Принципом целенаправленности;

c) Принципом управляемости;
d) Принципом разумной достаточности.
7. К утечкам информации не относится:
a) Разглашение;
b) Несанкционированный доступ к информации;
c) Получение защищаемой информации разведками;
d) Недобросовестная конкуренция.
8. В модели целостности Кларка-Вилсона все содержащиеся в системе данные подразделяются на:
a) Субъекты и объекты;
b) Секретные и общедоступные данные;
c) Контролируемые и неконтролируемые элементы;
d) Доступные и недоступные элементы.
9. К моделям, реализующим дискреционную политику безопасности, не относится …
a) Модель Take-Grant;
b) Расширенная модель Take-Grant;
c) Модель Харисона-Руззо-Ульмана (HRU-модель);
d) Модель Белла-ЛаПадула.
10. Задача модели безопасности при проектировании защищенных автоматизированных
систем – ?
a) Защита от взлома методом грубой силы;
b) Авторизация субъектов доступа;
c) Обеспечение заданного уровня конфиденциальности;
d) Формальное доказательство соблюдения политики безопасности.
11. Произвольная операция над объектом O, реализуемая в субъекте S и зависящая от
a) Потоком информации;
b) Доступом;
c) Политикой безопасности;
d) Активностью субъекта.
12. Для добавления нового объекта в систему в модели безопасности Take-Grant используется команда:
a) Grant;
)Append;
c) Create;
d) Make.
13. Модель, в которой безопасность автоматизированной системы рассматривается с точки зрения возможности получения субъектом определённых прав к некоторому объекту – это …
a) Модель целостности;
b) Субъект-объектная модель;
c) Дискреционная модель;
d) Модель распределения прав доступа.
14. Для какой из моделей безопасности характерны правила post, spy, find и pass?
a) Модель Take-Grant;
b) Расширенная модель Take-Grant;
c) Модель Харисона-Руззо-Ульмана (HRU-модель);
d) Модель Белла-ЛаПадула.
15. Модель Биба часто называют инверсией модели Белла-ЛаПадулла, потому что … a) Модели описывают различные политики безопасности;
b) Данные модели противоречат друг другу;

c) Основные правила моделей являются инверсными, но описывают разные уровни безопасности;
d) Исследователь не может применить данные модели одновременно.
16. Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, доступности информации в автоматизированной системе называется …
a) Компьютерной безопасностью; b) Угрозой безопасности;
c) Анализом угроз;
d) Атакой на информационную систему.
17. Под оцениванием угроз понимается …
a) Определение множества угроз, характерных, актуальных для конкретной компьютерной
системы;
b) Присвоение угрозам уникальных идентификаторов и описания;
c) Формирование оценок угроз с точки зрения потерь, ущерба, возможных от их реализации
d) Составление требований к обеспечению информационной безопасности компьютерной
системы.
18. По степени преднамеренности проявления угрозы делятся на …
a) Преднамеренного действия и случайного действия;
d) Формальное доказательство соблюдения политики безопасности.
11. Произвольная операция над объектом O, реализуемая в субъекте S и зависящая от
a) Потоком информации;
b) Доступом;
c) Политикой безопасности;
d) Активностью субъекта.
12. Для добавления нового объекта в систему в модели безопасности Take-Grant используется команда:
a) Grant; b) Append; c) Create; d) Make.
13. Модель, в которой безопасность автоматизированной системы рассматривается с точки зрения возможности получения субъектом определённых прав к некоторому объекту – это …
a) Модель целостности;
b) Субъект-объектная модель;
c) Дискреционная модель;
d) Модель распределения прав доступа.
14. Для какой из моделей безопасности характерны правила post, spy, find и pass?
a) Модель Take-Grant;
b) Расширенная модель Take-Grant;
c) Модель Харисона-Руззо-Ульмана (HRU-модель);
d) Модель Белла-ЛаПадула.
15. Модель Биба часто называют инверсией модели Белла-ЛаПадулла, потому что …
a) Модели описывают различные политики безопасности;
b) Данные модели противоречат друг другу;
c) Основные правила моделей являются инверсными, но описывают разные уровни безопасности;
d) Исследователь не может применить данные модели одновременно.
16. Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, доступности информации в автоматизированной системе называется …
a) Компьютерной безопасностью;

b) Угрозой безопасности;
c) Анализом угроз;
d) Атакой на информационную систему.
17. Под оцениванием угроз понимается …
a) Определение множества угроз, характерных, актуальных для конкретной компьютерной
системы;
b) Присвоение угрозам уникальных идентификаторов и описания;
c) Формирование оценок угроз с точки зрения потерь, ущерба, возможных от их реализации
d) Составление требований к обеспечению информационной безопасности компьютерной
системы.
18. По степени преднамеренности проявления угрозы делятся на …
a) Преднамеренного действия и случайного действия;
b) Естественной природы и искусственной природы;
c) Субъективного проявления и объективного проявления;
d) Пассивного действия и активного действия.
19. Основным (-и) фактором (-ами) оценки угрозы являются:
a) Возможность реализации угрозы и оценка возможного ущерба;
b) Оценка ценности объекта и стоимость средств защиты;
c) Идентификация воздействия угрозы на объект защиты;
d) Субъективная оценка возможности реализации угрозы.
20. Угроза применения «троянских» программ актуальна для систем с …
a) Мандатной политикой безопасности;
b) Контролем порождения субъектов и объектов; c) Дискреционной политикой безопасности;
d) Внедренным контролем целостности.
21. Активные угрозы …
a) Проявляются после разрешения доступа к ресурсам;
b) Проявляются независимо от активности компьютерной системы;
c) Вызваны воздействиями на компьютерную систему объективных физических процессов или стихийных природных явлений, не зависящих от человека;
d) При воздействии вносят изменения в структуру и содержание компьютерной системы.
22. Существование информации в неизменном виде по отношению к некоторому фиксированному ее состоянию обозначается свойством …
a) Конфиденциальности информации;
b) Целостности информации;
c) Доступности информации;
d) Актуальности информации.
23. Недостаток системы, используя который можно нарушить её безопасность, называется
a) Угроза;
b) Ошибка;
c) Недекларированные возможности;
d) Уязвимость.
24. Набор норм, правил и практических приемов, регулирующих управление, защиту и распространение ценной информации, называется …
a) Моделью безопасности;
b) Методом шифрования;
c) Компьютерной безопасностью;

d) Политикой безопасности.

25. Какая из мер не способна влиять на уровень безопасности парольной системы защиты?

a) Проверка и отбраковка пароля по словарю;

b) Введение двухфакторной аутентификации;

c) Ограничение числа попыток ввода пароля;

d) Установление минимального срока действия пароля.

26. Территория вокруг помещений автоматизированной системы, которая непрерывно контролируется персоналом или средствами компьютерной системы называется …

a) Внешняя неконтролируемая зона;

b) Зона контролируемой территории;

c) Зона помещений компьютерной системы;

d) зона ресурсов компьютерной системы.

27. Для какой политики безопасности характерно использование грифов секретности?

a) Для мандатной политики безопасности;

b) Для дискреционной политики безопасности;

c) И для мандатной, и для дискреционной политик безопасности; d) Ни для одной из политик безопасности.

28. Процедура распознавания субъекта по его идентификатору называется …

a) Идентфикацией;

b) Аутентификацией;

c) Авторизацией;

d) Регистрацией.

29. Принцип непрерывности в эксплуатации защищенных автоматизированных систем заключается в том, что …

a) Защитые механизмы системы должны функционировать в любых ситуациях, в том числе и внештатных;

b) Меры защиты должны быть направлены против перечня угроз, характерных для конкретной системы в конкретных условиях ее эксплуатации;

c) Подсистема безопасности системы должна строиться как система управления;

d) Необходимо использовать защитные механизмы различной и наиболее целесообразной в конкретных условиях природы.

30. Совокупность объектов, к которым разрешен доступ конкретному субъекту называется …

a) Политикой безопасности; b) Доменом безопасности;

c) Принципом управляемости; d) Субъект-объектной моделью.

31. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на ...

a) Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

b) Реализацию права на доступ к информации;

c) Разработку методов и усовершенствование средств информационной безопасности;

d) Выявление нарушителей и привлечение их к ответственности.

32. К мерам защиты информации в информационной системе не относится: a) Идентификация и аутентификация субъектов доступа и объектов доступа; b) Управление доступом субъектов доступа к объектам доступа;

c) Повышение эффективности работы вычислительной техники системы;

d) Защита информационной системы, ее средств и систем связи и передачи данных.

33. Меры защиты информации, выбираемые для реализации в автоматизированной системе, должны обеспечивать…

a) Блокирование одной или нескольких угроз безопасности информации, включенных в модель угроз безопасности информации;
b) Формирование модели угроз и модели нарушителя информационной системы; c) Анализ рисков информационной безопасности информационной системы;
d) Минимизацию затрат для поддержания уровня безопасности.

34. К методам повышения достоверности входных данных относится:
a) Замена процесса ввода значения процессом выбора значения из предлагаемого множества;
b) Отказ от использования данных;
c) Проведение комплекса регламентных работ;
d) Многократный ввод данных и сличение введенных значений.

35. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …
a) Несанкционированного управления удаленным компьютером;
b) Внедрения агрессивного программного кода в рамках активных объектов Web-страниц;
c) Перехвата или подмены данных на путях транспортировки;
d) Вмешательства в личную жизнь.

36. Утечка информации – это …
a) Несанкционированный процесс переноса информации от источника к злоумышленнику;
b) Процесс раскрытия секретной информации;
c) Процесс уничтожения информации;
d) Непреднамеренная утрата носителя информации.

37. Концепция системы защиты от информационного оружия не должна включать…
a) Механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры;
b) Признаки, сигнализирующие о возможном нападении;
c) Средства нанесения контратаки;
d) Процедуры оценки атаки против национальной инфраструктуры в целом и отдельных пользователей.

38. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на функционирование системы:
a) Активная; b) Пассивная;
c) Непреднамеренная; d) Естественная.

6.4.Вопросы для проверки остаточных знаний по дисциплине «Теоретические основы компьютерной безопасности»

1. Основные положения теории защиты информации.
2. Математическое моделирование в проектировании защищённых телекоммуникационных систем.
3. Классификация угроз безопасности информации в телекоммуникационных системах и их элементах.
4. Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем.
5. Мандатное разграничение доступа для обеспечения безопасности телекоммуникационных систем.
6. Ролевое разграничение доступа для обеспечения безопасности телекоммуникационных систем.
7. Изолированная программная среда в проектировании защищённых телекоммуникационных систем и их элементов.

7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Согласовано
Зав. библиотекой ФГБОУ ВО «ДГТУ»

№п\п	Виды занятий	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.ЛБ. СРС	Основы информационной безопасности	Галатенко В. А.	М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2013.	3	1
2.	ЛЗ.ЛБ. СРС	Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс]: учебное пособие для вузов. —	Девянин П.Н.	М. : Горячая линия-Телеком, 2013	http://e.lanbook.com/book/63235	
3.	ЛЗ.ЛБ. СРС	Основы информационной безопасности [Электронный ресурс]	Галатенко В. А.	М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 c. — 978-5-94774-821-5.	http://www.iprbookshop.ru/52209.html	
4.	ЛЗ.ЛБ. СРС	Теоретические основы компьютерной безопасности: учебное пособие	Мещеряков Р.В	Томск: В-Спектр, 2007. — 343 с.	-	1
5	ЛЗ.ЛБ. СРС	Основы информационной безопасности [Электронный ресурс]	Сычев, Ю. Н.	М.: Евразийский открытый институт, 2010. — 328 c. — 978-5-374-00381-9.	http://www.iprbookshop.ru/10746.html	
Дополнительная литература						
6.	ЛЗ.ЛБ. СРС	Основы информационной безопасности при работе на компьютере [Электронный ресурс]	Фаронов, А. Е.	М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 c. — 2227-8397.	http://www.iprbookshop.ru/52160.html	
7.	ЛЗ.ЛБ. СРС	Основы информационной безопасности [Электронный ресурс]	Голиков, А. М.	Томск: Томский государственный университет систем	http://www.iprbookshop.ru/13957.html	

				управления и радиоэлектроники, 2017. — 288 с. — 978-5-868889-467-1		
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,ЛБ, СРС	http://www.edu.ru - веб-сайт системы федеральных образовательных порталов				
10.	ЛЗ,ЛБ, СРС	http://www.sec.ru – каталог организаций в сфере информационной безопасности				
11.	ЛЗ,ЛБ, СРС	базы данных, информационно-справочные и поисковые системы: правовые справочно-поисковые системы («Гарант», «Консультант Плюс»), www.fstec.ru:www.gost.ru/wps/portal/tk362.				

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 факультете компьютерных технологий, вычислительной техники и энергетики имеется аудитория, оборудованная интерактивной доской, проектором, что позволяет читать лекции в формате презентаций, разработанных с помощью пакета прикладных программ MS Power Point, 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 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

Мустафа М.Г. Мирзаджанов

подпись ИОФ