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

ОДОБРЕНО
Методической комиссией по укрупненной группе специальностей и направлений 10.00.00 «Информационная безопасность»
Председатель МК:

_____ **Мелехин В.Б.**
Подпись ФИО

«17» 10 2018 г.

УТВЕРЖДАЮ:

Декан, председатель совета факультета КТВТиЭ,

_____ **Юсуфов Ш.А.**
Подпись
ФИО

«15» 10 2018г.

Фонд оценочных средств

по дисциплине «Теоретические основы компьютерной безопасности» для контроля знаний обучающихся специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем»

Составитель, ст. преп. _____ Качаева Г.И.

Фонд оценочных средств обсужден на заседании кафедры «Информационная безопасность» «15»10 2018г., протокол № 2

Зав. кафедрой _____ Качаева Г.И.

Фонд оценочных средств является приложением к рабочей программе по дисциплине С1.В.ОД.7 «Теоретические основы компьютерной безопасности»

Махачкала, 2018г.

Оглавление

1. Перечень компетенций с указанием этапов их формирования в процессе освоения ООП

1.1. Перечень компетенций и планируемые результаты

Табл.1

№	Содержание и код компетенций по ФГОС	В результате изучения дисциплины «Теоретические основы компьютерной безопасности» обучающиеся должны:		
		знать	уметь	владеть
1	способностью проводить анализ защищенности автоматизированных систем (ПК-3)	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	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	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

1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Теоретические основы компьютерной безопасности» определяется на следующих трех этапах:

1. Этап текущих аттестаций (вх.контр., текущие аттестации 1-3; СРС)
2. Этап промежуточных аттестаций

Таблица 2

Код компетенций по ФГОС	Этапы формирования компетенций по дисциплине «Теоретические основы компьютерной безопасности»					
	СЕМЕСТРЫ					
	I	II	III	VI		V
	-	-	-	Этап текущих аттестаций	Этап промеж.аттест.	-

	-	-	-	1 нед.	2-5нед.	6-10 нед.	11-15нед.	1-17 нед.	18-20нед.	-
	-	-	-	Входной контроль	Текущая аттест.1 (контр.раб. 1)	Текущая аттест.2 (контр.раб.2)	Текущая аттест.3 (контр.раб.3)	СРС	Промеж.аттест.	-
1	2	3	4	5	6	7	8	9	11	12
ПК-3	-	-	-	+	+	+	+	+	+	+

СРС – самостоятельная работа студентов; КР– курсовая работа; Знак «+» соответствует формированию компетенции.

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания.

В рамках текущих аттестаций (таблица 2) оценка уровня сформированности компетенций проводится на занятиях:

- лекционного типа посредством экспресс-опроса обучаемых, в том числе по темам и разделам, вынесенных для самостоятельного изучения;
- лабораторного типа путем устного опроса выполненных лабораторных заданий;
- практического типа методами проведения письменных контрольных работ.

Оценка сформированности компетенций в рамках промежуточной аттестации проводится по билетам для зачета. Они включают в себя вопросы для оценки знаний, умений и навыков, т.е. задания:

- *репродуктивного уровня,* позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умения правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины;
- *реконструктивного уровня,* позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей;
- *творческого уровня,* позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.

В ходе проведения текущей и промежуточной аттестации оцениваются:

- полнота и содержательность ответа;
- умение привести примеры из области операционных систем;
- умение пользоваться дополнительной литературой и современными технологиями обучения при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций, учебной литературы, интернет- ресурсам и другим источникам информации.

В ходе проведения оценки сформированности компетенций рекомендуются применение современных компьютерных технологий и виртуальных форм опроса в интерактивном режиме.

2.1. Описание показателей оценивания компетенций

Таблица 3

Оценка «неудовлетворительно» (не зачтено) или отсутствие сформированности компетенции	Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Оценка «отлично» (зачтено) или высокий уровень освоения компетенции
Неспособность обучаемого самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения, отсутствие самостоятельности в применении умения к использованию методов освоения учебной дисциплины и неспособность самостоятельно проявить навык повторения решения поставленной задачи по стандартному образцу свидетельствуют об отсутствии сформированной компетенции. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах освоения учебной дисциплины. Уровень освоения дисциплины, при котором у обучаемого не сформировано	Если обучаемый демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем, следует считать, что компетенция сформирована, но ее уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне. При наличии более 50% сформированных компетенций по дисциплинам, имеющим возможность доформирования компетенций на последующих этапах обучения. Для дисциплин итогового формирования	Способность обучающегося продемонстрировать самостоятельное применение знаний, умений и навыков при решении заданий, аналогичных тем, которые представлял преподаватель при потенциальном формировании компетенции, подтверждает наличие сформированной компетенции, причем на более высоком уровне. Наличие сформированной компетенции на повышенном уровне самостоятельности со стороны обучаемого при ее практической демонстрации в ходе решения аналогичных заданий следует оценивать как положительное и устойчиво закрепленное в практическом навыке. Для определения уровня освоения промежуточной дисциплины на оценку «хорошо» обучающийся должен продемонстрировать наличие 80% сформированных	Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий в рамках учебной дисциплины с использованием знаний, умений и навыков, полученных как в ходе освоения данной учебной дисциплины, так и смежных дисциплин, следует считать компетенцию сформированной на высоком уровне. Присутствие сформированной компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой адаптивности практического применения к изменяющимся условиям профессиональной задачи. Оценка «отлично» по дисциплине с промежуточным освоением компетенций, может быть выставлена при 100% подтверждении наличия компетенций, либо при 90%

более 50% компетенций. Если же учебная дисциплина выступает в качестве итогового этапа формирования компетенций (чаще всего это дисциплины профессионального цикла) оценка «неудовлетворительно» должна быть выставлена при отсутствии сформированности хотя бы одной компетенции.	компетенций естественно выставлять оценку «удовлетворительно», если сформированы все компетенции и более 60% дисциплин профессионального цикла «удовлетворительно».	компетенций, из которых не менее 1/3 оценены отметкой «хорошо». Оценивание итоговой дисциплины на «хорошо» обуславливается наличием у обучаемого всех сформированных компетенций причем общепрофессиональных компетенции по учебной дисциплине должны быть сформированы не менее чем на 60% на повышенном уровне, то есть с оценкой «хорошо».	сформированных компетенций, из которых не менее 2/3 оценены отметкой «хорошо». В случае оценивания уровня освоения дисциплины с итоговым формированием компетенций оценка «отлично» может быть выставлена при подтверждении 100% наличия сформированной компетенции у обучаемого, выполнены требования к получению оценки «хорошо» и освоены на «отлично» не менее 50% общепрофессиональных компетенций.

2.2. Описание критериев определения уровня сформированности компетенций

Таблица 4

Уовни сформированности компетенций	Критерии определения уровня сформированности	Компеенции, формируемые в результате освоения дисциплины ООП
		Профессиональные компетенции (ПК)
		ПК-3
Пороговый уровень	Компетенция сформирована	+
	Демонстрируется недостаточный уровень самостоятельности навыка	
	Обладает качеством **репродукции**	
Достаточный уровень	Компетенция сформирована	+
	Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка	
	Обладает качеством **реконструкции**	
Высокий уровень	Компетенция сформирована	+
	Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка	
	Обладает **творческим** качеством	

2.3. Описание шкал оценивания

В Дагестанском государственном техническом университете внедрена модульно-рейтинговая система оценки учебной деятельности студентов. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

Таблица 5

Шкалы оценивания			Критерии оценивания
пятибальная	двадцатибальная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 баллов	Показывает высокий уровень сформированности компетенций, т.е.: – продемонстрирует глубокое и прочное усвоение материала; – исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; – правильно формирует определения; – демонстрирует умения самостоятельной работы с нормативно-правовой литературой; – умеет делать выводы по излагаемому материалу.
«Хорошо» - 4 баллов	«Хорошо» - 15 -17 баллов	«Хорошо» - 70-84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: – демонстрирует достаточно полное знание материала, основных теоретических положений; – достаточно последовательно, грамотно логически стройно излагает материал; – демонстрирует умения ориентироваться в нормальной литературе; – умеет делать достаточно обоснованные выводы по излагаемому материалу.
«Удовлетворительно» - 3 баллов	«Удовлетворительно» - 12-14 баллов	«Удовлетворительно» - 56-69баллов	Показывает пороговый уровень сформированности компетенций, т.е.: – демонстрирует общее знание изучаемого материала; – испытывает серьезные затруднения при ответах на дополнительные вопросы; – знает основную рекомендуемую литературу; – умеет строить ответ в соответствии со структурой излагаемого материала.
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: – незнания значительной части программного материала; – невладения понятийным аппаратом дисциплины; – допущения существенных ошибок при изложении учебного материала; – неумение строить ответ в соответствии со структурой излагаемого вопроса; – неумение делать выводы по излагаемому материалу.

2.4. Определение уровня сформированности компетенций в результате изучения дисциплины «Теоретические основы компьютерной безопасности»

Таблица 6

№	Код компетенций по ФГОС	Уровни сформированности компетенций		
		Пороговый	Достаточный	Высокий
1	2	3	4	5
1	ПК-3	**Знает** 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 **(на пороговом уровне, или на « удовлетворительно»).** **Умеет** 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	**Знает** 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 **на достаточном уровне («на «хорошо»).** **Умеет** 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	**Знает** 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 **полноценно (на высоком уровне, на «отлично»).** **Умеет** 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**слабо.** **Владеет** 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**слабо.**	информации в АС в соответствии со стандартами по оценке защищенности АС**на достаточном уровне.** **Владеет** 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**на достаточном уровне.**	информации в АС в соответствии со стандартами по оценке защищенности АС**полноценно.** **Владеет** 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**полноценно.**

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения ООП.

3.1. Задания для входного контроля

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

3.2 Вопросы для текущих контрольных работ.

3.2.1 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.

3.2.2 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.

3.2.3 Аттестационная контрольная работа №3

1. Понятие роли.
2. Модель ролевого разграничения доступа.
3. Монитор безопасности объектов.
4. Монитор безопасности.
5. Изолированная программная среда.
6. Настройка DNS-клиентов.
7. Настройка параметров DNS-сервера.
8. Настройка свойств зоны и передачи.

3.3 Перечень вопросов на зачет

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»..

3.4 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) Идентификацией;

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.

3.4 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.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций.

В качестве методического материала рекомендуется использовать:
1. Положение о ФОС в ФГБОУ ВО «Дагестанский государственный технический университет» (Приложение № 9 к ООП).
2. Положение ФГБОУ ВО «Дагестанский государственный технический университет» о модульно-рейтинговой системе оценки учебной деятельности студентов.
3. Процедура проведения оценочных мероприятий.

4.1. Процедура проведения оценочных мероприятий

4.1.1. Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля (текущей аттестации) можно отнести устный опрос, письменные задания, контрольные работы.

Основные этапы текущего контроля:

– в конце каждой лекции или лабораторного занятия студентам выдаются задания для внеаудиторного выполнения по соответствующей теме;
– срок выполнения задания устанавливается по расписанию занятий (к очередной лекции или лабораторному занятию);

– студентам, пропускающим занятия, выдаются дополнительные задания – представить конспект пропущенного занятия, написанный «от руки» с последующим собеседованием по теме занятия;

– подведение итогов контроля проводится по графику проведения текущего контроля;

– результаты оценки успеваемости заносятся в рейтинговую ведомость и доводятся до сведения студентов;

К достоинствам данного типа относится его систематичность, непосредственно коррелирующаяся с требованием постоянного и непрерывного мониторинга качества обучения, а также возможность бально-рейтинговой оценки успеваемости обучающихся.

Недостатком является фрагментарность и локальность проверки. Компетенцию целиком, а не отдельные ее элементы (знания, умения, навыки) при подобном контроле проверить невозможно.

4.1.2.Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов).

Промежуточная аттестация помогает оценить более крупные совокупности знаний и умений, в некоторых случаях – даже формирование определенных профессиональных компетенций.

Достоинства: помогает оценить более крупные совокупности знаний и умений, в некоторых случаях – даже формирование определенных профессиональных компетенций.

Форма промежуточной аттестации: **зачет**.

Текущий контроль и промежуточная аттестация традиционно служат основным средством обеспечения в учебном процессе «обратной связи» между преподавателем и обучающимся, необходимой для стимулирования работы обучающихся и совершенствования методики преподавания учебных дисциплин.

Основные этапы промежуточной аттестации:

- зачет проводится по расписанию сессии;
- форма проведения занятия – письменная контрольная работа;
- вид контроля – фронтальный;
- требование к содержанию контрольной работы – дать краткий ответ на поставленный вопрос (задание);
- итоговая оценка определяется как сумма оценок, полученных в текущей аттестации и по результатам написания контрольной работы;
- проверка ответов и объявление результатов производится в день написания контрольной работы;
- результаты аттестации заносятся в зачетную книжку студента .

Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

При первой попытке ликвидации задолженности, во время зачетной недели или в течение сессии, студенту выдаются все задания по текущему контролю и промежуточной аттестации, по которым он не смог набрать зачетное количество баллов.

При ликвидации задолженности после сессии студенту выдаются для выполнения все задания по текущему контролю, кроме аналитического обзора, если он выполнен ранее, и вопросы зачетного занятия промежуточной аттестации, включая дополнительные вопросы по теме аналитического обзора.