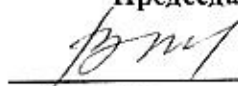


Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»
Кафедра «Информационная безопасность»


ОДОБРЕНО

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


Подпись Мелехин В.Б.
ФИО
«17» 10 2018 г.

УТВЕРЖДАЮ:

Декан, председатель совета
факультета КТВТиЭ,


Подпись Юсупов Ш.А.
ФИО
«19» 10 2018 г.

Фонд оценочных средств

по дисциплине «Комплексное обеспечение информационной безопасности автоматизированных систем» 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.9 «Комплексное обеспечение информационной безопасности автоматизированных систем»

Махачкала, 2018г.

Оглавление

1. Перечень компетенций с указанием этапов их формирования в процессе освоения ООП	3
1.1. Перечень компетенций и планируемые результаты	3
1.2. Этапы формирования компетенций.....	4
2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания	6
2.1. Описание показателей оценивания компетенций	7
2.2. Описание критериев определения уровня сформированности компетенций	9
2.3. Описание шкал оценивания.....	10
2.4. Определение уровня сформированности компетенций в результате изучения дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем»	11
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.....	15
3.1. Задания для входного контроля	15
3.2. Вопросы для текущих контрольных работ.....	15
3.2.1. Аттестационная контрольная работа №1	15
3.2.2. Аттестационная контрольная работа №2	15
3.2.3. Аттестационная контрольная работа №3	16
3.3. Перечень вопросов на экзамен.....	16
3.4. Вопросы для проверки остаточных знаний по дисциплине «Комплексное обеспечение информационной безопасности автоматизированных систем».....	17
4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций.	17
4.1. Процедура проведения оценочных мероприятий	17

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 «Комплексное обеспечение информационной безопасности автоматизированных систем» обучающиеся должны:			
		знать	уметь	владеть	
1	способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5)	концептуальные основы комплексного обеспечения информационной безопасности автоматизированных систем	выявлять возможные нарушения безопасности при автоматизированных обработки информации	способы информационной работе систем	навыками решать задачи и программно-аппаратными средствами и давать оценку качества предлагаемых решений
2	способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8)	общие методологические принципы комплексных систем обеспечения информационной безопасности	применять криптографические решения для защиты информации и квалифицированно оценивать их качество	стандартные решения для информации	навыками системный подход к обеспечению информационной безопасности в различных сферах деятельности
3	способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11)	основные методы и средства проектирования систем обеспечения информационной безопасности	оценивать модели и политику безопасности	основные методы и средства систем проектирования информационной безопасности	навыками проектировать и реализовывать комплексную систему защиты информации, оценивать ее качество
4	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной	методы оценки качества систем и моделей; об определении и измерении параметров опасных сигналов для технических каналов утечки информации и определять эффективность защиты	реализовывать системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем	способы защиты документов в области информационной безопасности	навыками работы с нормативными документами в области информационной безопасности

5	системы (ПК-12) способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13)	от утечки информации действующие стандарты, требования и нормативную базу в области защиты информации	развертывать комплексную систему защиты информации в автоматизированных системах	подходами к проектированию и внедрению комплекса защитных мер в автоматизированных системах
6	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14)	основные принципы и методы создания комплексного обеспечения информационной безопасности автоматизированных систем	строить политики безопасности автоматизированных систем в соответствии с критериями и требованиями нормативных документов	навыками проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации
7	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17)	действующие стандарты, требования и нормативную базу в области защиты информации	проводить инструментальный мониторинг защищенности информации	навыками проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации

1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Комплексное обеспечение информационной безопасности автоматизированных систем» определяется на следующих трех этапах:

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

Таблица 2

Этапы формирования компетенций по дисциплине «Комплексное обеспечение информационной безопасности автоматизированных систем»				
СЕМЕСТРЫ				
VIII				
Код компетенций по ФГОС	I	II	III	Этап
	-	-	-	Этап
				V
				-

				промеж. аттес						
				1 нед. Входной контроль	2-5 нед. Текущая аттест.1 (контр. раб. 1)	6-10 нед. Текущая аттест.2 (контр. раб.2)	11-15 нед. Текущая аттест.3 (контр. раб.3)	1-17 нед. СРС	18-20 нед. Промеж. аттес Т. (экзамен)	-
1	2	3	4	5	6	7	8	9	11	12
ПК-5	-	-	-	+	+	+	+	+	+	+
ПК-8	-	-	-	+	+	+	+	+	+	+
ПК-11	-	-	-	+	+	+	+	+	+	+
ПК-12	-	-	-	+	+	+	+	+	+	+
ПК-13	-	-	-	+	+	+	+	+	+	+
ПК-14	-	-	-	+	+	+	+	+	+	+
ПК-17	-	-	-	+	+	+	+	+	+	+

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 низкий уровень освоения компетенции	Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Оценка «отлично» (зачтено) или высокий уровень освоения компетенции
<p>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 обучаемого не сформировано</p>	<p>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</p>	<p>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</p>	<p>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%</p>

<p>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.</p>	<p>компетенций естественно выставлять оценку «удовлетворительно», если сформированы все компетенции и более 60% дисциплин профессионального цикла «удовлетворительно».</p>	<p>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».</p>	<p>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.</p>
---	--	--	---

2.2. Описание критериев определения уровня сформированности компетенций

Таблица 4

Уровни сформированности компетенций	Критерии определения уровня сформированности	Компетенции, формируемые в результате освоения дисциплины ООП							
		Профессиональные компетенции (ПК)							
		ПК-5	ПК-8	ПК-11	ПК-12	ПК-12	ПК-13	ПК-14	ПК-17
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 пятибалльная, двадцатибалльная и стобалльная шкалы знаний, умений, навыков.

Таблица 5

Шкалы оценивания			Критерии оценивания
пятибалльная	двадцатибалльная	стобалльная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 баллов	Показывает высокий уровень сформированности компетенций, т.е.: <ul style="list-style-type: none"> - демонстрирует 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.: <ul style="list-style-type: none"> - 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» - 56-69 баллов	Показывает пороговый уровень сформированности компетенций, т.е.: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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 «Комплексное обеспечение информационной безопасности автоматизированных систем»

Таблица 6

		Уровни сформированности компетенций		
№	Код компетенций по ФГОС	Пороговый	Достаточный	Высокий
		3	4	5
1	ПК-5	<p>Знает концептуальные основы комплексного обеспечения информационной безопасности автоматизированных систем (на пороговом уровне, или на «удовлетворительно»).</p> <p>Умеет выявлять возможные способы нарушения информационной безопасности при работе автоматизированных систем обработки информации слабо.</p> <p>Владет навыками практически решать задачи защиты программ и данных программно-аппаратными средствами и давать оценку качества предлагаемых решений слабо.</p>	<p>Знает концептуальные основы комплексного обеспечения информационной безопасности автоматизированных систем на достаточном уровне («на хорошо»).</p> <p>Умеет выявлять возможные способы нарушения информационной безопасности при работе автоматизированных систем обработки информации на достаточном уровне.</p> <p>Владет навыками практически решать задачи защиты программ и данных программно-аппаратными средствами и давать оценку качества предлагаемых решений на достаточном уровне.</p>	<p>Знает концептуальные основы комплексного обеспечения информационной безопасности автоматизированных систем полноценно (на высоком уровне, на «отлично»).</p> <p>Умеет выявлять возможные способы нарушения информационной безопасности при работе автоматизированных систем обработки информации полноценно.</p> <p>Владет навыками практически решать задачи защиты программ и данных программно-аппаратными средствами и давать оценку качества предлагаемых решений полноценно.</p>
2	ПК-8	<p>Знает общие методологические принципы комплексных систем обеспечения информационной безопасности (на пороговом уровне, или на «удовлетворительно»).</p>	<p>Знает общие методологические принципы комплексных систем обеспечения информационной безопасности на достаточном уровне («на хорошо»).</p> <p>Умеет</p>	<p>Знает общие методологические принципы комплексных систем обеспечения информационной безопасности полноценно (на высоком уровне, на «отлично»).</p>

		<p>Умеет применять стандартные криптографические решения для защиты информации и квалифицированно оценивать их качество слабо.</p> <p>Владеет навыками применять системный подход к обеспечению информационной безопасности в различных сферах деятельности слабо</p>	<p>навыками применять системный подход к обеспечению информационной безопасности в различных сферах деятельности на достаточном уровне.</p> <p>Владеет навыками применять системный подход к обеспечению информационной безопасности в различных сферах деятельности на достаточном уровне.</p>	<p>Умеет применять системный подход к обеспечению информационной безопасности в различных сферах деятельности полноценно.</p> <p>Владеет навыками применять системный подход к обеспечению информационной безопасности в различных сферах деятельности полноценно.</p>
3	ПК-11	<p>Знает основные методы и средства проектирования систем обеспечения информационной безопасности (на пороговом уровне, или на «удовлетворительно»).</p> <p>Умеет оценивать модели и политику безопасности слабо.</p> <p>Владеет навыками проектировать и реализовывать комплексную систему защиты информации, оценивать ее качество слабо.</p>	<p>Знает основные методы и средства проектирования систем обеспечения информационной безопасности на достаточном уровне («на хорошо»).</p> <p>Умеет оценивать модели и политику безопасности на достаточном уровне.</p> <p>Владеет навыками проектировать и реализовывать комплексную систему защиты информации, оценивать ее качество на достаточном уровне.</p>	<p>Знает основные методы и средства проектирования систем обеспечения информационной безопасности (на высоком уровне, на «отлично»).</p> <p>Умеет оценивать модели и политику безопасности полноценно.</p> <p>Владеет навыками проектировать и реализовывать комплексную систему защиты информации, оценивать ее качество полноценно.</p>
4	ПК-12	<p>Знает методы оценки качества систем и моделей; об определении и измерении параметров опасных сигналов для технических каналов утечки информации и определять эффективность защиты от утечки информации (на</p>	<p>Знает методы оценки качества систем и моделей; об определении и измерении параметров опасных сигналов для технических каналов утечки информации и определять эффективность защиты от утечки информации (на</p>	<p>Знает методы оценки качества систем и моделей; об определении и измерении параметров опасных сигналов для технических каналов утечки информации и определять эффективность защиты от утечки информации (на</p>

		<p>пороговом уровне, или на «удовлетворительно»). Умеет реализовывать системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем слабо. Владеет навыками работы с нормативными документами в области информационной безопасности слабо.</p>	<p>информация достаточном уровне (она «хорошо»). Умеет реализовывать системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем на достаточном уровне. Владеет навыками работы с нормативными документами в области информационной безопасности на достаточном уровне.</p>	<p>высоком уровне, на «отлично»). Умеет реализовывать системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем полноценно. Владеет навыками работы с нормативными документами в области информационной безопасности полноценно.</p>
5	ПК-13	<p>Знает действующие стандарты, требования и нормативную базу в области защиты информации (на пороговом уровне, или на «удовлетворительно»). Умеет развертывать комплексную систему защиты информации в автоматизированных системах слабо. Владеет подходами к проектированию и внедрению комплекса защитных мер в автоматизированных системах слабо.</p>	<p>Знает действующие стандарты, требования и нормативную базу в области защиты информации на достаточном уровне (она «хорошо»). Умеет развертывать комплексную систему защиты информации в автоматизированных системах на достаточном уровне. Владеет подходами к проектированию и внедрению комплекса защитных мер в автоматизированных системах на достаточном уровне.</p>	<p>Знает действующие стандарты, требования и нормативную базу в области защиты информации полноценно (на «отлично»). Умеет развертывать комплексную систему защиты информации в автоматизированных системах полноценно. Владеет подходами к проектированию и внедрению комплекса защитных мер в автоматизированных системах полноценно.</p>
6	ПК-14	<p>Знает основные принципы и методы создания комплексного обеспечения информационной безопасности</p>	<p>Знает основные принципы и методы создания комплексного обеспечения информационной безопасности</p>	<p>Знает основные принципы и методы создания комплексного обеспечения информационной безопасности</p>

	<p>автоматизированных систем (на пороговом уровне, или на «удовлетворительно»).</p> <p>Умеет</p> <p>строить политики безопасности автоматизированных систем в соответствии с критериями и требованиями нормативных документов слабо.</p> <p>Владеет</p> <p>навыками проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации слабо.</p>	<p>автоматизированных систем на достаточном уровне («на «хорошо»).</p> <p>Умеет</p> <p>строить политики безопасности автоматизированных систем в соответствии с критериями и требованиями нормативных документов на достаточном уровне.</p> <p>Владеет</p> <p>навыками проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации на достаточном уровне.</p>	<p>автоматизированных систем полноценно (на высоком уровне, на «отлично»).</p> <p>Умеет</p> <p>строить политики безопасности автоматизированных систем в соответствии с критериями и требованиями нормативных документов полноценно.</p> <p>Владеет</p> <p>навыками проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации полноценно.</p>
7	<p>ПК-17</p> <p>Знает</p> <p>действующие стандарты, требования и нормативную базу в области защиты информации (на пороговом уровне, или на «удовлетворительно»).</p> <p>Умеет</p> <p>проводить инструментальный мониторинг защищенности информации слабо.</p> <p>Владеет</p> <p>навыками проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации слабо.</p>	<p>Знает</p> <p>действующие стандарты, требования и нормативную базу в области защиты информации на достаточном уровне («на «хорошо»).</p> <p>Умеет</p> <p>проводить инструментальный мониторинг защищенности информации на достаточном уровне.</p> <p>Владеет</p> <p>навыками проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации на достаточном уровне.</p>	<p>Знает</p> <p>действующие стандарты, требования и нормативную базу в области защиты информации полноценно (на высоком уровне, на «отлично»).</p> <p>Умеет</p> <p>проводить инструментальный мониторинг защищенности информации полноценно.</p> <p>Владеет</p> <p>навыками организации и проведении навыками проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации полноценно.</p>

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. 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. Рольное разграничение доступа для обеспечения безопасности телекоммуникационных систем.
7. Изолированная программная среда в проектировании защищённых телекоммуникационных систем и их элементов.

3.2 Вопросы для текущих контрольных работ.

3.2.1 Аттестационная контрольная работа №1

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

3.2.2 Аттестационная контрольная работа №2

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

3.2.3 Аттестационная контрольная работа №3

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

3.3 Перечень вопросов на экзамен

1. Информационная сфера и информационная среда.
2. Виды защищаемой информации.
3. Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации.
4. Виды угроз информационной безопасности объекту защиты и их характеристика.
5. Модель нарушителя информационной безопасности.
6. Модель угрозы информационной безопасности.
7. Структура сил и средств организационной защиты информации.
8. Функции, задачи и особенности службы безопасности организации.
9. Принципы организации службы безопасности организации.
10. Типовая структура службы безопасности.
11. Основные документы, регламентирующие деятельность службы безопасности объекта.
12. Участие сотрудников в организационной защите информации.
13. Взаимодействие службы безопасности объекта с правоохранительными органами.
14. Обеспечение режима секретности при проведении НИОКР по секретной (конфиденциальной) тематике, при разработке и изготовлении изделий, их опытной эксплуатации и серийном производстве.
15. Требования режима секретности при работе с секретными документами.
16. Назначение и задачи секретного делопроизводства.
17. Порядок разработки, учета, хранения, размножения и уничтожения секретных (конфиденциальных) документов.
18. Понятия допуска к секретной (конфиденциальной) информации и доступа к (конфиденциальным) работам, документам и изделиям.
19. Формы допусков.
20. Служебное расследование нарушений режима секретности.
21. Организация работ по защите информации при опубликовании открытых материалов.
22. Подсистема контроля доступа и аудита.
23. Подсистема администрирования безопасности.
24. Назначение и требования внутриобъектового режима.
25. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации.
26. Требования к помещениям, в которых циркулирует защищаемая информация.
27. Понятие пропускного режима.
28. Цели и задачи пропускного режима.
29. Организация пропускного режима.
30. Атрибутные и биометрические идентификаторы людей.
31. Порядок оформления и выдачи пропусков.
32. Оценка ущерба и анализ рисков информационной безопасности.

33. Оценка затрат на организацию и проведение мероприятий по обеспечению информационной безопасности.
34. Порядок организации информационной безопасности объекта при осуществлении международного научнотехнического и экономического сотрудничества.
35. Основные требования, предъявляемые к подготовке служебного совещания.
36. Организация обеспечения режима секретности при проведении служебного совещания.
37. Требования к помещениям для проведения совещания.

3.4 Вопросы для проверки остаточных знаний по дисциплине «Комплексное обеспечение информационной безопасности автоматизированных систем»

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

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:

- экзамен 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);
- количество вопросов в экзаменационном билете;
- 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 экзаменационную ведомость и зачетную книжку студента (при получении экзамена).

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.