


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 \_\_\_\_\_ Юсуфов Ш.А.  
ФИО \_\_\_\_\_  
«18» 10 2018 г.

Фонд оценочных средств

по дисциплине «Разработка и эксплуатация защищенных АС» для контроля знаний обучающихся специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем»

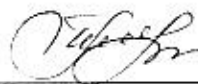
Составитель, ст. преп.



Качасва Г.И.

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

Зав. кафедрой



Качасва Г.И.

Фонд оценочных средств является приложением к рабочей программе по дисциплине С1.Б.31. «Разработка и эксплуатация защищенных АС»

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 .....	5
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 «Разработка и эксплуатация защищенных АС».....	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. ....	16
3.1. Задания для входного контроля .....	16
3.2 Вопросы для текущих контрольных работ. ....	16
3.2.1 Аттестационная контрольная работа №1 .....	16
3.2.2 Аттестационная контрольная работа №2 .....	16
3.2.3 Аттестационная контрольная работа №3 .....	17
3.3 Перечень вопросов на экзамен.....	17
3.4 Вопросы для проверки остаточных знаний по дисциплине «Разработка и эксплуатация защищенных АС».....	18
4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций. ....	18
4.1. Процедура проведения оценочных мероприятий .....	19

1. Перечень компетенций с указанием этапов их формирования в процессе освоения ООП  
1.1. Перечень компетенций и планируемые результаты

Табл.1

В результате изучения дисциплины «Разработка и эксплуатация защищенных АС» обучающиеся должны:		знать	уметь	владеть
№	Содержание и код компетенций по ФГОС			
1	способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5)	принципы и методы построения защищенных автоматизированных систем	классифицировать защищаемую информацию по видам тайны и уровням конфиденциальности	навыками создания АС в соответствии с ГОСТ 34.XXX
2	способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8)	механизмы, используемые для защиты информации, циркулирующей в различных системах	классифицировать и оценивать угрозы информационной безопасности для объекта информатизации	навыками подготовки технического задания на разработку системы защиты информации
3	способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9)	основные информационные технологии, используемые в автоматизированных системах	формировать комплекс мер по защите информации в АС и оценивать их эффективность на основе заданных требований по безопасности информации	навыками подготовки системы к аттестации
4	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12)	основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические)	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации	классифицировать АС по уровню защищенности

5	способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13)	автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	участвовать в проектировании средств защиты информации автоматизированной системы	навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем
6	способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20)	методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем	разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем	навыками анализа основных узлов и устройств современных автоматизированных систем; навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем
7	способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25)	содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем	восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях	методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; навыками анализа и синтеза структурных функциональных защищенных автоматизированных информационных систем
8	способностью управлять информационной безопасностью автоматизированной системы (ПК-28)	методы, способы и средства обеспечения отказоустойчивости автоматизированных систем	выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности	навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности

### 1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Разработка и эксплуатация защищенных АС» 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 «Разработка и эксплуатация защищенных АС»										
Код компетенций по ФГОС	СЕМЕСТРЫ									
	VIII									
	I	II	III	Этап текущих аттестаций						Этап промежуточных аттестаций
			1 нед.	2-5нед.	6-10 нед.	11-15нед.	1-17 нед.	18-20нед.	т.	-
1	2	3	4	5	6	7	8	9	11	12
	-	-	-	+	+	+	+	+	+	+
ПК-5	-	-	-	+	+	+	+	+	+	+
ПК-8	-	-	-	+	+	+	+	+	+	+
ПК-9	-	-	-	+	+	+	+	+	+	+
ПК-12	-	-	-	+	+	+	+	+	+	+
ПК-13	-	-	-	+	+	+	+	+	+	+
ПК-20	-	-	-	+	+	+	+	+	+	+
ПК-25	-	-	-	+	+	+	+	+	+	+
ПК-28	-	-	-	+	+	+	+	+	+	+

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 способность 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</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 представил 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 выстает 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-9	ПК-12	ПК-13	ПК-20	ПК-25	ПК-28
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"> <li>- демонстрирует глубокое и прочное усвоение материала;</li> <li>- исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал;</li> <li>- правильно формирует определения;</li> <li>- демонстрирует умения самостоятельной работы с нормативно-правовой литературой;</li> <li>- умеет делать выводы по излагаемому материалу.</li> </ul>
«Хорошо» - 4 баллов	«Хорошо» - 15 -17 баллов	«Хорошо» - 70-84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: <ul style="list-style-type: none"> <li>- демонстрирует достаточно полное знание материала, основных теоретических положений;</li> <li>- достаточно последовательно, грамотно логически стройно излагает материал;</li> <li>- демонстрирует умения ориентироваться в нормальной литературе;</li> <li>- умеет делать достаточно обоснованные выводы по излагаемому материалу.</li> </ul>
«Удовлнительно» - 3 баллов	«Удовлнительно» - 12-14 баллов	«Удовлнительно» - 56-69 баллов	Показывает пороговый уровень сформированности компетенций, т.е.: <ul style="list-style-type: none"> <li>- демонстрирует общее знание изучаемого материала;</li> <li>- испытывает серьезные затруднения при ответах на дополнительные вопросы;</li> <li>- знает основную рекомендуемую литературу;</li> <li>- умеет строить ответ в соответствии со структурой излагаемого материала.</li> </ul>
«Неудовлнительно» - 2 баллов	«Неудовлнительно» - 1-11 баллов	«Неудовлнительно» - 1-55 баллов	Ставится в случае: <ul style="list-style-type: none"> <li>- незнания значительной части программного материала;</li> <li>- невладения понятийным аппаратом дисциплины;</li> <li>- допущения существенных ошибок при изложении учебного материала;</li> <li>- неумение строить ответ в соответствии со структурой излагаемого вопроса;</li> <li>- неумение делать выводы по излагаемому материалу.</li> </ul>

2.4. Определение уровня сформированности компетенций в результате изучения дисциплины «Разработка и эксплуатация защищенных АС»

Таблица 6

№	Код компетенций по ФГОС	Уровни сформированности компетенций		
		Пороговый	Достаточный	Высокий
1	ПК-5	3	4	5
1	ПК-5	<p>Знает принципы и методы построения защищенных автоматизированных систем (на пороговом уровне, или на «удовлетворительно»).</p> <p>Умеет классифицировать защищаемую информацию по видам тайны и уровням конфиденциальности слабо.</p> <p>Владет навыками создания АС слабо.</p>	<p>Знает принципы и методы построения защищенных автоматизированных систем на достаточном уровне («на хорошо»).</p> <p>Умеет классифицировать защищаемую информацию по видам тайны и уровням конфиденциальности на достаточном уровне.</p> <p>Владет навыками создания АС на достаточном уровне.</p>	<p>Знает принципы и методы построения защищенных автоматизированных систем полноценно (на высоком уровне, на «отлично»).</p> <p>Умеет классифицировать защищаемую информацию по видам тайны и уровням конфиденциальности полноценно.</p> <p>Владет навыками создания АС полноценно.</p>
2	ПК-8	<p>Знает механизмы, используемые для защиты информации, циркулирующей в различных системах (на пороговом уровне, или на «удовлетворительно»).</p> <p>Умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации слабо.</p> <p>Владет навыками подготовки технического</p>	<p>Знает механизмы, используемые для защиты информации, циркулирующей в различных системах на достаточном уровне («на хорошо»).</p> <p>Умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации на достаточном уровне.</p> <p>Владет навыками подготовки технического</p>	<p>Знает механизмы, используемые для защиты информации, циркулирующей в различных системах полноценно (на высоком уровне, на «отлично»).</p> <p>Умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации полноценно.</p> <p>Владет навыками подготовки технического задания на разработку системы</p>

		задания на разработку системы защиты информации слабо.	задания на разработку системы защиты информации на достаточном уровне.	защиты информации полноценно.
3	ПК-9	<p>Знает основные информационные технологии, используемые в автоматизированных системах (на пороговом уровне, или на «удовлетворительно»).</p> <p>Умеет формировать комплекс мер по защите информации в АС и оценивать их эффективность на основе заданных требований по безопасности информации слабо.</p> <p>Владеет навыками подготовки системы к аттестации слабо.</p>	<p>Знает основные информационные технологии, используемые в автоматизированных системах на достаточном уровне («хорошо»).</p> <p>Умеет формировать комплекс мер по защите информации в АС и оценивать их эффективность на основе заданных требований по безопасности информации на достаточном уровне.</p> <p>Владеет навыками подготовки системы к аттестации на достаточном уровне.</p>	<p>Знает основные информационные технологии, используемые в автоматизированных системах (на высоком уровне, на «отлично»).</p> <p>Умеет формировать комплекс мер по защите информации в АС и оценивать их эффективность на основе заданных требований по безопасности информации полноценно.</p> <p>Владеет навыками подготовки системы к аттестации полноценно.</p>
4	ПК-12	<p>Знает основные меры по защите информации в автоматизированных системах (на пороговом уровне, или на «удовлетворительно»).</p> <p>Умеет разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации слабо.</p> <p>Владеет классифицировать АС по уровню защищенности слабо.</p>	<p>Знает основные меры по защите информации в автоматизированных системах на достаточном уровне («хорошо»).</p> <p>Умеет разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на достаточном уровне.</p> <p>Владеет классифицировать АС по уровню защищенности на достаточном уровне.</p>	<p>Знает основные меры по защите информации в автоматизированных системах (на высоком уровне, на «отлично»).</p> <p>Умеет разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации полноценно.</p> <p>Владеет классифицировать АС по уровню защищенности полноценно.</p>
5	ПК-13	Знает	Знает	Знает

6	<p>автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности (на пороговом уровне, или на «удовлетворительно»).</p> <p>Умеет участвовать в проектировании средств защиты информации автоматизированной системы слабо.</p> <p><b>Владеет</b> навыками выбора и обоснования критериев функционирования защищенных автоматизированных информационных систем слабо.</p>	<p>автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности на достаточном уровне («на «хорошо»).</p> <p>Умеет участвовать в проектировании средств защиты информации автоматизированной системы на достаточном уровне.</p> <p><b>Владеет</b> навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем на достаточном уровне.</p>	<p>автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности, на «отлично»).</p> <p>Умеет участвовать в проектировании средств защиты информации автоматизированной системы полноценно.</p> <p><b>Владеет</b> навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем полноценно.</p>
ПК-20	<p><b>Знает</b> методы, способы, средства, последовательность и содержание этапов разработки систем и безопасности систем (на пороговом уровне, или на «удовлетворительно»).</p> <p>Умеет разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем слабо.</p>	<p><b>Знает</b> методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности систем на достаточном уровне («на «хорошо»).</p> <p>Умеет разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем на достаточном уровне.</p> <p><b>Владеет</b></p>	<p><b>Знает</b> методы, способы, средства, последовательность и содержание этапов разработки систем и безопасности систем автоматизированных систем полноценно (на высоком уровне, на «отлично»).</p> <p>Умеет разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем</p>

	<p><b>Владеет</b> навыками анализа основных узлов и устройств современных систем; навыками автоматизированных систем; навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных средств аппаратных системемлабо.</p>	<p>навыками анализа основных узлов и устройств современных систем; навыками автоматизированных работоспособности, поддержания и устранения неисправностей в работе электронных средств аппаратных системемлабо.</p>	<p><b>полноценно.</b> <b>Владеет</b> навыками анализа основных узлов и устройств современных систем; навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем</p>
7	<p><b>Знает</b> содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем (на пороговом уровне, или на «удовлетворительно»).</p> <p><b>Умеет</b> восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нестандартных ситуациях слабо.</p> <p><b>Владеет</b> методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных</p>	<p><b>Знает</b> содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем на достаточном уровне («на «хорошо»).</p> <p><b>Умеет</b> восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нестандартных ситуациях на достаточном уровне.</p> <p><b>Владеет</b> методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных</p>	<p><b>Знает</b> содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем <b>полноценно (на высоком уровне, на «отлично»).</b></p> <p><b>Умеет</b> восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нестандартных ситуациях <b>полноценно.</b></p> <p><b>Владеет</b> методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; навыками анализа и синтеза</p>

8	ПК-28	<p>автоматизированных информационных систем <b>слабо</b>.</p> <p><b>Знает</b> методы, способы и средства обеспечения отказоустойчивости автоматизированных систем (на пороговом уровне, или на «удовлетворительно»).</p> <p><b>Умеет</b> выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем <b>слабо</b>.</p> <p><b>Владет</b> навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности <b>слабо</b>.</p>	<p>автоматизированных информационных систем на <b>достаточном уровне</b>.</p> <p><b>Знает</b> методы, способы и средства обеспечения отказоустойчивости автоматизированных систем на <b>достаточном уровне</b> («на «хорошо»»).</p> <p><b>Умеет</b> выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем на <b>достаточном уровне</b>.</p> <p><b>Владет</b> навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности на <b>достаточном уровне</b>.</p>	<p>структурных и функциональных схем защищенных автоматизированных информационных систем <b>полноценно</b>.</p> <p><b>Знает</b> методы, способы и средства обеспечения отказоустойчивости автоматизированных систем <b>полноценно</b> (на высоком уровне, на «отлично»).</p> <p><b>Умеет</b> выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем <b>полноценно</b>.</p> <p><b>Владет</b> навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности <b>полноценно</b>.</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. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?

**3.2 Вопросы для текущих контрольных работ.**

**3.2.1 Аттестационная контрольная работа №1**

1. Введение. Составление технического задания на автоматизированные информационные системы.
2. Понятие качества и эффективности: характеристики качества, показатели и критерии эффективности, методические вопросы оценки эффективности сложных систем. Функциональная и обеспечивающая часть сложной системы.
1. Понятие сложной системы: элементы и подсистемы, управление и информация, самоорганизация.
2. Методы проектирования сложных систем.
3. Методология построения автоматизированных систем.
4. Уровни проектирования.
5. Структуризация предметной области, построение ее инфологической модели.
6. Основные этапы проектирования, их особенности.
7. Основные объекты проектирования: их классификация и характеристики.
8. Структурный подход к проектированию сложных систем.
9. Проектирование автоматизированных информационных систем.
10. Содержание работ на этапах создания автоматизированных информационных систем.
11. Принципы построения защищенных информационных систем.
12. Содержание работ на этапах создания автоматизированных информационных систем.
1. Комплекс стандартов на автоматизированные системы.

**3.2.2 Аттестационная контрольная работа №2**

1. Методы построения обобщенных критериев.
2. Экспертные методы оценок критериев.
3. Анализ характеристик системы управления на основе информационного графа.
4. Вычисление структурно – топологических характеристик систем управления.
5. Вычисление числовых характеристик системы управления с помощью задания числовой функции на структурном графе системы.
6. Способы описания структурного сопряжения элементов.
7. Распределение задач управления по узлам.
8. Основные принципы системного подхода при создании сложных систем.
9. Технология функционирования сложной системы.
10. Средства автоматизации проектирования автоматизированных информационных систем.



11. ГОСТ 19.701-90 (ИСО 5807-85) «ЕСПД Схемы алгоритмов, программ данных и систем».
12. ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности Условные обозначения».
13. Оценочные уровни доверия и классификации автоматизированных систем.
14. Средства построения пользовательского интерфейса.
15. Средства разработки программно-информационного ядра информационных систем.

### 3.2.3 Аттестационная контрольная работа №3

1. Разработка политики безопасности.
2. Настройка прав доступа к объектам БД в СУБД.
3. Настойка регистрации системны событий средствами СУБД.
4. Защита от несанкционированного доступа к информации.
5. Технологии работы ядра безопасности, мониторов обращений и прочих компонентов, позволяющих обеспечить безопасность создаваемого программного комплекса.
6. Типовые пр-фили защиты автоматизированных систем
7. Тестирование автоматизированных информационных систем.
8. ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».
9. Подготовка приложения к распространению.
10. Принципы документального процесса сопровождения автоматизированной системы.

### 3.3 Перечень вопросов на экзамен

1. Составление технического задания на автоматизированные информационные системы.
2. Понятие качества и эффективности: характеристики качества, показатели и критерии эффективности, методические вопросы оценки эффективности сложных систем. Функциональная и обеспечивающая часть сложной системы.
13. Понятие сложной системы: элементы и подсистемы, управление и информация, самоорганизация.
14. Методы проектирования сложных систем.
15. Методология построения автоматизированных систем.
16. Уровни проектирования.
17. Структуризация предметной области, построение ее инфологической модели.
18. Основные этапы проектирования, их особенности.
19. Основные объекты проектирования: их классификация и характеристики.
20. Структурный подход к проектированию сложных систем.
21. Проектирование автоматизированных информационных систем.
22. Содержание работ на этапах создания автоматизированных информационных систем.
23. Принципы построения защищенных информационных систем.
24. Содержание работ на этапах создания автоматизированных информационных систем.
25. Комплекс стандартов на автоматизированные системы.
3. Методы построения обобщенных критериев.
4. Экспертные методы оценок критериев.
5. Анализ характеристик системы управления на основе информационного графа.
6. Вычисление структурно – топологических характеристик систем управления.
7. Вычисление числовых характеристик системы управления с помощью задания числовой функции на структурном графе системы.
8. Способы описания структурного сопряжения элементов.
9. Распределение задач управления по узлам.
10. Основные принципы системного подхода при создании сложных систем.
11. Технология функционирования сложной системы.

12. Средства автоматизации проектирования автоматизированных информационных систем.
13. ГОСТ 19.701-90 (ИСО 5807-85) «ЕСПД Схемы алгоритмов, программ данных и систем».
14. ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности Условные обозначения».
15. Оценочные уровни доверия и классификации автоматизированных систем.
16. Средства построения пользовательского интерфейса.
  1. Средства разработки программно-информационного ядра информационных систем
  2. Разработка политики безопасности.
  3. Настройка прав доступа к объектам БД в СУБД.
  4. Настойка регистрации системных событий средствами СУБД.
  5. Программная реализация механизма регистрации доступа к полям и строкам таблицы. Разработка подсистемы идентификации и установление подлинности пользователя и программного продукта.
  6. Защита от несанкционированного доступа к информации.
  7. Технологии работы ядра безопасности, мониторов обращений и прочих компонентов, позволяющих обеспечить безопасность создаваемого программного комплекса.
  8. Типовые профили защиты автоматизированных систем
  9. Тестирование автоматизированных информационных систем.
  10. ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».
  11. Подготовка приложения к распространению.
  12. Принципы документального процесса сопровождения автоматизированной системы.
  13. Ввод в эксплуатацию автоматизированных информационных систем.
  14. ГОСТ 19.505-79 «Руководство оператора. Требования к содержанию и оформлению». Определение ключевых различий между руководствами программиста и администратора. Рассмотрение примеров документации.
  15. Обобщение результатов изучения предыдущих этапов.
  16. Автоматизированные системы на этапе эксплуатации, условий вывода из эксплуатации.
  17. Эксплуатация автоматизированных информационных систем.
  18. Требования к управлению информационной безопасностью и восстановлению систем после сбоя.

#### **3.4 Вопросы для проверки остаточных знаний по дисциплине «Разработка и эксплуатация защищенных АС»**

1. Угрозы безопасности компьютерных систем.
2. Обобщение результатов изучения предыдущих этапов.
3. Автоматизированные системы на этапе эксплуатации, условий вывода из эксплуатации.
4. Эксплуатация автоматизированных информационных систем.
5. Требования к управлению информационной безопасностью и восстановлению систем после сбоя.
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 балльно-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.