

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 «Информационно-аналитические работы по обеспечению информационной безопасности автоматизированных систем» для контроля знаний обучающихся специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализации «Безопасность открытых информационных систем»

Составитель



Качасва Г.И.

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

Зав. кафедрой



Качасва Г.И.

Фонд оценочных средств является приложением к рабочей программе по дисциплине С1.В.ДВ.4 «Информационно-аналитические работы по обеспечению информационной безопасности автоматизированных систем»

Махачкала, 2018 г.

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.....	3
2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания.	5
2.1. Описание показателей оценивания компетенций	6
2.2. Описание критериев определения уровня сформированности компетенций	8
2.3. Описание шкал оценивания.....	9
2.4. Определение уровня сформированности компетенций в результате изучения дисциплины «Информационно-аналитические работы по обеспечению информационной безопасности автоматизированных систем»	10
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.....	12
3.1. Задания для входного контроля	12
3.2 Вопросы для текущих контрольных работ	12
3.2.1 Аттестационная контрольная работа №1	12
3.2.1 Аттестационная контрольная работа №2	12
3.2.3 Аттестационная контрольная работа №3	13
3.3 Перечень вопросов на экзамен	13
.....	15
3.4 Вопросы для проверки остаточных знаний по дисциплине «Информационно-аналитические работы по обеспечению информационной безопасности автоматизированных систем»	15
Способы определения нарушений информационной безопасности.....	15
4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций	15
4.1. Процедура проведения оценочных мероприятий	15
4.1.1. Текущий контроль	15
4.1.2.Промежуточная аттестация.....	16

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 «Информационно-аналитические работы по обеспечению информационной безопасности автоматизированных систем» обучающиеся должны:		
		знать	уметь	владеть
1	способностью разрабатывать модели угроз и модели нарушителя информации модели безопасности автоматизированной системы (ПК-4)	базовые понятия современных методов оценки безопасности компьютерных систем	выявлять угрозы и определять их актуальность для современных компьютерных систем; описывать (моделировать) объекты защиты и угрозы безопасности компьютерных систем	практическими навыками применения методов обеспечения безопасности компьютерных систем
2	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6)	проблемы обеспечения безопасности информации, решаемые с применением современных методов и средств защиты информации (ЗИ) в компьютерных системах	применять наиболее эффективные методы обеспечения безопасности компьютерных систем	методами формирования требований по защите информации
3	способностью участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы (ПК-4.4)	принципы и способы использования существующих средств ЗИ в компьютерных системах	применять современные Информационно-аналитические работы по обеспечению ИБАС	навыками применения современных методов оценки безопасности компьютерных систем

1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Информационно-аналитические работы по обеспечению 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

Код компетенций по ФГОС	Этапы формирования компетенций по дисциплине «Информационно-аналитические работы по обеспечению информационной безопасности автоматизированных систем»					
	I		II-VIII		IX	
	СЕМЕСТРЫ		СЕМЕСТРЫ		СЕМЕСТРЫ	
		1 нед.	2-5 нед.	18-20 нед.		X
		Входной контроль	Текущая аттест.1 (контр. раб. 1)	Промеж. аттест.		
1	2	4	5	6		
ПК-4	-	+	+	+		7
ПК-6	-	+	+	+		+
ПСК-4.4	-	+	+	+		+

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 экзамена. 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
<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 использованно методов освоения учебной дисциплины и способность самостоятельно проявить навыки 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 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-4	ПК-5	ПСК-4.4
Пороговый	Компетенция сформирована	+	+	+
	Демонстрируется недостаточный уровень самостоятельности навыка			
	Обладает качеством репродукции			
Достаточный	Компетенция сформирована	+	+	+
	Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка			
	Обладает качеством реконструкции			
Высокий	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"> - 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.: <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 «Информационно-аналитические ра-
боты по обеспечению информационной безопасности автоматизированных систем»

		Уровни сформированности компетенций		
№	Код компетенций по ФГОС	Пороговый	Достаточный	Высокий
1	2	3	4	5
1	ПК-4	<p>Знает базовые понятия современных методов оценки безопасности компьютерных систем (на пороговом уровне, или на «удовлетворительно»).</p> <p>Умеет выявлять угрозы и определять их актуальность для современных компьютерных систем; описывать (моделировать) объекты защиты и угрозы безопасности компьютерных систем слабо.</p> <p>Владеет практическими навыками применения методов обеспечения безопасности компьютерных систем слабо.</p>	<p>Знает базовые понятия современных методов оценки безопасности компьютерных систем на достаточном уровне («на «хорошо»).</p> <p>Умеет выявлять угрозы и определять их актуальность для современных компьютерных систем; описывать (моделировать) объекты защиты и угрозы безопасности компьютерных систем на достаточном уровне.</p> <p>Владеет практическими навыками применения методов обеспечения безопасности компьютерных систем</p>	<p>Знает базовые понятия современных методов оценки безопасности компьютерных систем полноценно (на высоком уровне, на «отлично»).</p> <p>Умеет выявлять угрозы и определять их актуальность для современных компьютерных систем; описывать (моделировать) объекты защиты и угрозы безопасности компьютерных систем полноценно.</p> <p>Владеет практическими навыками применения методов обеспечения безопасности компьютерных систем полноценно.</p>
2	ПК-6	<p>Знает проблемы обеспечения безопасности информации, решаемые с применением современных методов и средств защиты информации (ЗИ) в компьютерных системах (на пороговом уровне, или на «удовлетворительно»).</p> <p>Умеет применять наиболее эффективные методы обеспечения безопасности компьютерных систем слабо.</p> <p>Владеет методами формирования требований по защите информации слабо.</p>	<p>Знает проблемы обеспечения безопасности информации, решаемые с применением современных методов и средств защиты информации (ЗИ) в компьютерных системах на достаточном уровне («на «хорошо»).</p> <p>Умеет применять наиболее эффективные методы обеспечения безопасности компьютерных систем на достаточном уровне.</p> <p>Владеет методами формирования требований по защите информации на достаточном уровне.</p>	<p>Знает проблемы обеспечения безопасности информации, решаемые с применением современных методов и средств защиты информации (ЗИ) в компьютерных системах полноценно (на высоком уровне, на «отлично»).</p> <p>Умеет применять наиболее эффективные методы обеспечения безопасности компьютерных систем полноценно.</p> <p>Владеет методами формирования требований по защите информации полноценно.</p>

Таблица 6

3	ПСК-4.4	<p>Знает принципы и способы использования существующих средств ЗИ в компьютерных системах (на пороговом уровне, или на «удовлетворительно»).</p> <p>Умеет применять современные Информационно-аналитические работы по обеспечению ИБАС слабо.</p> <p>Владет навыками применения современных методов оценки безопасности компьютерных систем слабо.</p>	<p>Знает принципы и способы использования существующих средств ЗИ в компьютерных системах на достаточном уровне («на «хорошо»).</p> <p>Умеет применять современные Информационно-аналитические работы по обеспечению ИБАС на достаточном уровне.</p> <p>Владет навыками применения современных методов оценки безопасности компьютерных систем на достаточном уровне.</p>	<p>Знает принципы и способы использования существующих средств ЗИ в компьютерных системах полноценно (на высоком уровне, на «отлично»).</p> <p>Умеет применять современные Информационно-аналитические работы по обеспечению ИБАС полноценно.</p> <p>Владет навыками применения современных методов оценки безопасности компьютерных систем 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. Ролевое 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. Основные понятия. Модель нарушителя.
2. Организационно-правовые вопросы защиты информации
3. Защита информации от ПЭМИН.
4. Каналы утечки информации из компьютерных систем.
5. Пассивные и активные методы защиты
6. Основы криптографии.
7. Понятия и определения; классификация шифров.
8. Блочные и поточные шифры.
9. Основы теории защиты информации в компьютерных системах.
10. Критерии информационной безопасности
11. Основные понятия теории защиты информации.
12. Угрозы безопасности; математические модели политики безопасности.
13. Общие критерии безопасности информационных технологий
14. Специфические особенности защиты информации в компьютерных сетях
15. Разделение совместно используемых ресурсов.
16. Расширение зоны контроля.
17. Комбинация различных программно-аппаратных средств.
18. Неизвестный периметр.
19. Множество точек атаки.
20. Сложность управления и контроля доступа к системе.
21. Средства защиты информации от НСД.
22. Способы несанкционированного доступа к информации и защиты от него в компьютерных системах

3.2.1 Аттестационная контрольная работа №2

1. Методы и средства защиты информационно-программного обеспечения на уровне операционных систем.
2. Классы защищенности СВТ от НСД.
3. Требования безопасности информации к операционным системам.

4. Профили защиты операционных систем.
5. Разграничение полномочий для групп и учетных записей пользователей.
6. Локальная групповая политика.
7. Применение симметричных криптосистем для защиты компьютерной информации.
8. Поля Фейстеля; стандарт шифрования данных DES.
9. Отечественный стандарт шифрования данных.
10. Технологии идентификации и аутентификации в компьютерных сетях.
11. идентификация и аутентификация.
12. Управление доступом.
13. Сервисы безопасности.
14. Методы защиты внешнего периметра компьютерных сетей.
15. Фильтры пакетов.
16. Шлюзы сеансового уровня.
17. Шлюзы прикладного уровня.
18. Межсетевые экраны экспертного уровня.
19. Системы обнаружения вторжений.
20. IDS уровня сети.
IDS уровня хоста.

3.2.3 Аттестационная контрольная работа №3

1. Безопасность компьютерных систем
2. Задачи информационной безопасности.
3. Конфиденциальность, целостность, доступность данных и программ.
4. Понятие политики безопасности.
5. Методы обеспечения информационной безопасности – криптография, модели безопасности, контроль поведения.
6. Программные уязвимости, виды уязвимостей.
7. Эксплуатация уязвимостей.
8. Инструменты.
9. Информация о процессах в системе.
10. Основы технологии виртуальных защищенных сетей VPN.
11. Технологии виртуальных защищенных сетей VPN.
12. Концепция построения виртуальных защищенных сетей VPN.
13. Основные понятие и функции сети VPN.
14. Методы реализации безопасности VPN.
15. Мероприятия по выявлению каналов утечки информации.
Специальные проверки. Порядок проведения специальной проверки технических средств.

3.3 Перечень вопросов на экзамен

1. Основные понятия. Модель нарушителя.
2. Организационно-правовые вопросы защиты информации
3. Защита информации от ПЭМИН.
4. Каналы утечки информации из компьютерных систем.
5. Пассивные и активные методы защиты
6. Основы криптографии.
7. Понятия и определения; классификация шифров.
8. Блочные и поточные шифры.
9. Основы теории защиты информации в компьютерных системах.
10. Критерии информационной безопасности
11. Основные понятия теории защиты информации.
12. Угрозы безопасности; математические модели политики безопасности.
13. Общие критерии безопасности информационных технологий
14. Специфические особенности защиты информации в компьютерных сетях
15. Разделение совместно используемых ресурсов.

16. Расширение зоны контроля.
17. Комбинация различных программно-аппаратных средств.
18. Неизвестный периметр.
19. Множество точек атаки.
20. Сложность управления и контроля доступа к системе.
21. Средства защиты информации от НСД.
22. Способы несанкционированного доступа к информации и защиты от него в компьютерных системах
23. Безопасность компьютерных систем
24. Задачи информационной безопасности.
25. Конфиденциальность, целостность, доступность данных и программ.
26. Понятие политики безопасности.
27. Методы обеспечения информационной безопасности – криптография, модели безопасности, контроль поведения.
28. Программные уязвимости, виды уязвимостей.
29. Эксплуатация уязвимостей.
30. Инструменты.
31. Информация о процессах в системе.
32. Методы и средства защиты информационно-программного обеспечения на уровне операционных систем.
33. Классы защищенности СВТ от НСД.
34. Требования безопасности информации к операционным системам.
35. Профили защиты операционных систем.
36. Разграничение полномочий для групп и учетных записей пользователей.
37. Локальная групповая политика.
38. Применение симметричных криптосистем для защиты компьютерной информации.
39. Поля Фейстеля; стандарт шифрования данных DES.
40. Отечественный стандарт шифрования данных.
41. Технологии идентификации и аутентификации в компьютерных сетях.
42. идентификация и аутентификация.
43. Управление доступом.
44. Сервисы безопасности.
45. Методы защиты внешнего периметра компьютерных сетей.
46. Фильтры пакетов.
47. Шлюзы сеансового уровня.
48. Шлюзы прикладного уровня.
49. Межсетевые экраны экспертного уровня.
50. Системы обнаружения вторжений.
51. IDS уровня сети.
52. IDS уровня хоста.
53. Основы технологии виртуальных защищенных сетей VPN.
54. Технологии виртуальных защищенных сетей VPN.
55. Концепция построения виртуальных защищенных сетей VPN.
56. Основные понятие и функции сети VPN.
57. Методы реализации безопасности VPN.
58. Мероприятия по выявлению каналов утечки информации.
59. Специальные проверки. Порядок проведения специальной проверки технических средств.
60. Технологии обнаружения вторжений в компьютерных сетях.
61. Способ сбора информации.
62. Метод анализа информации.
63. Способ реагирования на угрозы.
64. Требования к IDS.

65. Использование уязвимостей.
66. Тестирование систем IDS.
67. Методы идентификации и аутентификации пользователей компьютерных систем.
68. Аутентификация дапных.
69. Алгоритмы безопасного хширования.
70. ЭЦП криптосистем RSA и Эль Гамала.
71. Алгоритм цифровой подписи DSA; отечественные алгоритмы цифрой подписи.
72. Адаптивное управление безопасностью в компьютерных сетях.
73. Особенности современных подходов к анализу информационной безопасности.
74. Анализ методов функционирования современного Вредоносного программного обеспечения.
75. Способы определения нарушений информационной безопасности.

3.4 Вопросы для проверки остаточных знаний по дисциплине «Информационно-аналитические работы по обеспечению информационной безопасности автоматизированных систем»

1. Основные понятия. Модель нарушителя.
2. Безопасность компьютерных систем
3. Методы обеспечения информационной безопасности.
4. Основные понятия теории защиты информации.
5. Сложность управления и контроля доступа к системе.
6. Средства защиты информации от НСД.
7. Способы несанкционированного доступа к информации и защиты от него в компьютерных системах
8. Методы и средства защиты информационно-программного обеспечения на уровне операционных систем.
9. Классы защищенности СВТ от НСД.
10. Сервисы безопасности.
11. Методы защиты внешнего периметра компьютерных сетей.
12. Мероприятия по выявлению каналов утечки информации.
13. Алгоритм цифровой подписи DSA; отечественные алгоритмы цифрой подписи.
14. Адаптивное управление безопасностью в компьютерных сетях.
15. Особенности современных подходов к анализу информационной безопасности.
16. Анализ методов функционирования современного Вредоносного программного обеспечения.

Способы определения нарушений информационной безопасности

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: экзамен.

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 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 зачета).

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.