Приложение А

(обязательное к программе практической подготовки)

Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

Филиал в г. Дербенте

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине **«Информационная безопасность »**

Уровень образования бакалавриат

Направление подготовки 09.03.03 Прикладная информатика,

Профиль направления подготовки Прикладная информатика в экономике

Разработчик Е.Р. Джумалиева ст. преподаватель

Фонд оценочных средств обсужден на заседании кафедры ЕГО и СД «27»09 2022г., протокол №2

Зав. кафедрой С.Ф. Исмаилова

Дербент 2022 г.

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Информационная безопасность» и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. по самостоятельной работе студентов, далее – СРС), освоивших программу данной дисциплины.

Целью фонда оценочных средств является установление соответствия уровня подготовки обучающихся требованиям ФГОС ВО по направлению подготовки 09.03.03 – «Прикладная информатика».

Задачи фонда оценочных средств заключаются в контроле и оценке входных, текущих, промежуточных и остаточных знаний студента на соответствие их компетенциям, предусмотренным в рабочей программе дисциплины.

Рабочей программой дисциплины «Информационная безопасность» предусмотрено формирование следующих общепрофессиональных компетенций:

- ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности;
- ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;

Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)

1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП

1.1.1. Перечень компетенций и планируемые результаты

В результате освоения дисциплины «Информационная безопасность» обучающийся по направлению подготовки **09.03.03 – «Прикладная информатика» по профилю** подготовки – «Прикладная информатика в экономике», в соответствии с ФГОС ВО и ОПОП ВО должен обладать следующими компетенциями (см. таблицу 1):

Таблица 1- Компетенции обучающегося, формируемые в результате освоения дисциплины

Категория (группа) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
ОПК-3.	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

	информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
ОПК-4.	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знает основные стандарты оформления технической документации нараз-личных стадиях жизненного цикла информационной системы. ОПК-4.2. Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Информационная безопасность» определяется на следующих трех этапах:
1. **Этап текущих аттестаций** (текущие аттестации 1-3; СРС; КР)
2. **Этап промежуточных аттестаций** (диф. зачет)

Таблица 2 – Этапы формирования компетенций

Код компетенций по ФГОС	**Этапы формирования компетенций по дисциплине «Информационная безопасность»**					
	СЕМЕСТРЫ					
	VII					
	Этап текущих аттестаций				**Этап промеж.аттест.**	
	1-5 нед.	**6-10 нед.**	**11-15 нед.**	**1-17 нед.**	**18-20 нед.**	
	Текущая аттест.1 (контр.раб. 1)	Текущая аттест.2 (контр.раб.2)	Текущая аттест.3 (контр.раб.3)	СРС (творч.отчет)	КР (поясн.зап., ГМ)	Промеж.аттест. (зачет)
1	8	9	10	11	12	13
ОПК-3	+	+	+	+	-	+
ОПК-4	+	+	+	+	-	+

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

2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания

2.2.1. Показатели уровней сформированности компетенций на этапах их формирования

Результатом освоения дисциплины «Информационная безопасность»
является установление одного из уровней сформированности компетенций: высокий, повышенный, базовый, низкий.

Таблица 3

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
Высокий (оценка «отлично», «зачтено»)	Сформированы четкие системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные и верные. Даны развернутые ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции	Обучающимся усвоена взаимосвязь основныхпонятий дисциплины, в том числе для решения профессиональных задач. Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции
Повышенный (оценка «хорошо», «зачтено»)	Знания и представления по дисциплине сформированы на повышенном уровне. В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно подробное описание ответа, приведены и раскрыты в тезисной форме основные понятия. Ответ отражает полное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичные негрубые ошибки. Обучающимся продемонстрирован повышенный уровень освоения компетенции	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные. Продемонстрирован повышенный уровень владения практическими умениями и навыками. Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков
Базовый (оценка «удовлетворительно», «зачтено»)	Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП. Обучающийся допускает неточности в ответе, но	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки.

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
	обладает необходимыми знаниями для их устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции	Продемонстрирован базовый уровень владения практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач
Низкий (оценка «неудовлетворительно», «не зачтено»)	Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков	

Показатели уровней сформированности компетенций могут быть изменены, дополнены и адаптированы к конкретной рабочей программе дисциплины.

2.2.2. Описание шкал оценивания

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности студентов. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

Шкалы оценивания			**Критерии оценивания**
пятибальная	двадцатибальная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: – продемонстрирует глубокое и прочное усвоение материала; – исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; – правильно формирует определения; – демонстрирует умения самостоятельной работы с нормативно-правовой литературой; – умеет делать выводы по излагаемому материалу.
«Хорошо» - 4 баллов	«Хорошо» - 15 - 17 баллов	«Хорошо» - 70 - 84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: – демонстрирует достаточно полное знание материала, основных теоретических положений; – достаточно последовательно, грамотно логически стройно излагает материал; – демонстрирует умения ориентироваться в нормальной литературе; – умеет делать достаточно обоснованные выводы по излагаемому материалу.
«Удовлетворительно» - 3 баллов	«Удовлетворительно» - 12 - 14 баллов	«Удовлетворительно» - 56 – 69 баллов	Показывает пороговый уровень сформированности компетенций, т.е.: – демонстрирует общее знание изучаемого материала; – испытывает серьезные затруднения при ответах на дополнительные вопросы; – знает основную рекомендуемую литературу; – умеет строить ответ в соответствии со структурой излагаемого материала.
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: – незнания значительной части программного материала; – не владения 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.

2.2.3. Перечень компетенций с указанием этапов их формирования

Таблица 4 - Этапы формирования компетенций очной (заочной) формы обучения

Код компетенции	Этап формирования компетенции очной формы обучения (заочной формы обучения), семестры
ОПК-3	7 (7)
ОПК-4	7 (7)

2.2.4. Показатели и критерии оценивания компетенций

Таблица 5- Показатели компетенций по уровню их сформированности (зачет/экзамен)

Показатели компетенции (ий)	Критерий оценивания	Шкала оценивания	Уровень сформированной компетенции
Знать (соответствует таблице 1)	Знает	зачтено/отлично	высокий
		зачтено/хорошо	повышенный
		зачтено/удовлетворительно	пороговый
	Не знает	не зачтено/неудовлетворительно	недостаточный
Умеет (соответствует таблице 1)	Умеет	зачтено/отлично	высокий
		зачтено/хорошо	повышенный
		зачтено/удовлетворительно	пороговый
	Не умеет	не зачтено/неудовлетворительно	недостаточный
Владеть (соответствует таблице 1)	Владеет	зачтено/отлично	высокий
		зачтено/хорошо	повышенный
		зачтено/удовлетворительно	пороговый
	Не владеет	не зачтено/неудовлетворительно	недостаточный

Таблица 6 – Соотношение показателей и критериев оценивания компетенций со шкалой оценивания и уровнем их сформированности

Показатели компетенции (ий) (дескрипторы)	Критерий оценивания	Уровень сформированной компетенции
Знать (соответствует таблице 1)	Показывает полные и глубокие знания, логично и аргументированно отвечает на все вопросы, в том числе дополнительные, показывает высокий уровень теоретическихзнаний	высокий
	Показывает глубокие знания, грамотно излагает ответ, достаточно полно отвечает на все вопросы, в том числе дополнительные. В то же время при ответе допускает несущественные погрешности	повышенный
	Показывает достаточные, но не глубокие знания, при ответе не допускает грубых ошибок или противоречий, однако в формулировании ответа отсутствует должная связь между анализом, аргументацией и выводами. Для получения правильного ответа требуются уточняющие вопросы	пороговый
	Показывает недостаточные знания, не способен аргументированно и последовательно излагатьматериал, допускает грубые ошибки, неправильно отвечает на дополнительные вопросы или затрудняется с ответом	недостаточный
Уметь (соответствует таблице 1)	Умеет применять полученные знания для решения конкретных практических задач, способен предложить альтернативные решения анализируемых проблем, формулировать выводы	высокий
	Умеет применять полученные знания для решения конкретныхпрактическихзадач,способенформулировать выводы, но не может предложить альтернативные решения анализируемыхпроблем	повышенный
	При решении конкретных практических задач возникаютзатруднения	пороговый
	Не может решать практические задачи	недостаточный
Владеть (соответствует таблице 1)	Владеетнавыками,необходимымидляпрофессиональной деятельности, способен оценить результат своейдеятельности	высокий
	Владеет навыками, необходимыми для профессиональной деятельности, затрудняется оценить результатсвоейдеятельности	повышенный

	Показывает слабые навыки, необходимые дляпрофессиональной деятельности	пороговый
	Отсутствие навыков	недостаточный

2.2.5. Порядок аттестации обучающихся по дисциплине

Для аттестации обучающихся по дисциплине используется традиционная система оценки знаний.

По дисциплине «Информационная безопасность» в 7 семестре для очного и заочного обучения предусмотрен дифференцированный зачет. Оценивание обучающегося представлено в таблицах 7.

Таблица 7 – Применение системы оценки для проверки результатов итогового контроля – зачет

Оценка	Критерии оценки
«отлично»	имеет четкое представление о современных методах, методиках итехнологиях, применяемых в рамках изучаемойдисциплины; свободно и правильно оперирует предметной и методической терминологией; свободно владеет вопросами экзаменационного билета; подтверждает теоретические знания практическими примерами; дает развернутые ответы на задаваемые дополнительные вопросы; имеет собственные суждения о решении теоретических и практических вопросов, связанных с профессиональной деятельностью.
«хорошо»	имеет представление о современных методах, методиках и технологиях, применяемых в рамках изучаемой дисциплины; знает предметную и методическую терминологию дисциплины; излагает ответы на вопросы экзаменационного билета, ориентируясь на написанное им в экзаменационном листе; подтверждает теоретические знания отдельными практическими примерами; дает ответы на задаваемые дополнительные вопросы.
«удовлетворительно»	имеет посредственное представление о современных методах, методиках и технологиях, применяемых в рамках изучаемой дисциплины; правильно оперирует основными понятиями; отвечает на вопросы экзаменационного билета, главным образом, зачитывая написанное в экзаменационном листе; излагает, главным образом, теоретические знания по вопросам экзаменационногобилета; не во всех случаях находит правильные ответы на задаваемые дополнительныевопросы.

«неудовлетворительно»	не имеет представления о современных методах, методиках и технологиях, применяемых в рамках изучаемой дисциплины; не во всех случаях правильно оперирует основными понятиями; отвечает на экзаменационные вопросы, зачитывая их с экзаменационные вопросы излагает не в полной мере; не отвечает на дополнительные вопросы

2.2.6. Определение уровня сформированности компетенций в результате изучения дисциплины «Информационная безопасность»

Таблица 8 - Уровни сформированности компетенций

№	Код компетенций по ФГОС	Уровни сформированности компетенций		
		Пороговый	**Достаточный**	**Высокий**
1	2	3	4	5
	ОПК-3	**Знает** принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности**слабо (на пороговом уровне, или на « удовлетворительно»)** . **Умеет** решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом	**Знает** принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности**на достаточном уровне (на «хорошо»).** **Умеет** решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований	**Знает** принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности**полноценно (на высоком уровне, на «отлично»).** **Умеет** решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **полноценно.**

		основных требований информационной безопасности **слабо.** **Владеет** навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности **слабо.**	информационной безопасности **на достаточном уровне.** **Владеет** навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности **на достаточном уровне.**	**Владеет** навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности **полноценно.**
	ОПК-4	**Знает** основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы **слабо (на пороговом уровне, или на « удовлетворительно»).** **Умеет** применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы **слабо.** **Владеет** навыками составления технической документации на	**Знает** основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы **на достаточном уровне («на «хорошо»).** **Умеет** применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы **на достаточном уровне.** **Владеет** навыками составления технической	**Знает** основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы **полноценно (на высоком уровне, на «отлично»).** **Умеет** применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы **полноценно.** **Владеет** навыками составления технической документации на различных этапах жизненного цикла

		различных этапах жизненного цикла информационной системы **слабо.**	документации на различных этапах жизненного цикла информационной системы **на достаточном уровне.**	информационной системы **полноценно.**

3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП

ВОПРОСЫ ВХОДНОГО КОНТРОЛЯ

1.Основные понятия ИБ.
2.Информация,защищаемая информация, ценность информации, уровень секретности.
3.Объекты защиты информации.
4.Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.
5.Классификация угроз безопасности: каналы утечки, воздействия.
6.Прямые и косвенные каналы утечки данных.
7. Основы теории ИБ
8.Модель потенциального нарушителя.
9.Способы мошенничества в информационных системах. 3.Основные способы реализации угроз ИБ.
10.Основные понятия теории ИБ.
11. Оценка эффективности систем защиты информации
12.Принципы организации систем обеспечения безопасности данных.
13.Требования, предъявляемые к системам обеспечения безопасности данных.
14. Понятие мониторов безопасности. 4.Физические средства защиты Информации

ПЕРЕЧЕНЬ ВОПРОСОВ ТЕКУЩИХ КОНТРОЛЬНЫХ РАБОТ

Аттестационная контрольная № 1

1.Основные понятия ИБ.
2.Информация,защищаемая информация, ценность информации, уровень секретности.
3.Объекты защиты информации.
4.Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.
5.Классификация угроз безопасности: каналы утечки, воздействия.
6.Прямые и косвенные каналы утечки данных.
7. Основы теории ИБ
8.Модель потенциального нарушителя.
9.Способы мошенничества в информационных системах.
10.Основные способы реализации угроз ИБ.

Аттестационная контрольная № 2

1.Основные понятия теории ИБ.
2. Оценка эффективности систем защиты информации
3.Принципы организации систем обеспечения безопасности данных.

4.Требования, предъявляемые к системам обеспечения безопасности
данных.
5. Понятие мониторов безопасности.
6.Физические средства защиты
информации
7. Нормативные руководящие документы в сфере обеспечения ИБ

Аттестационная контрольная № 3
1. Понятие политики безопасности.
Дискреционные политики безопасности. Мандатные политики безопасности
2. Модель безопасности информационных потоков.
3.Показатели эффективности
систем защиты информации.
4.Способы оценки эффективности систем защиты информации.
5.Руководящие документы Гостехкомиссии в сфере обеспечения ИБ

Вопросы к зачету по дисциплине «Информационная безопасность»
1.Основные понятия ИБ.
2.Информация,защищаемая информация, ценность информации, уровень секретности.
3.Объекты защиты информации.
4.Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.
5.Классификация угроз безопасности: каналы утечки, воздействия.
6.Прямые и косвенные каналы утечки данных.
7. Основы теории ИБ
8.Модель потенциального нарушителя.
9.Способы мошенничества в информационных системах. 3.Основные способы
реализации угроз ИБ.
10.Основные понятия теории ИБ.
11. Оценка эффективности систем защиты информации
12.Принципы организации систем
обеспечения безопасности данных.
13.Требования, предъявляемые к системам обеспечения безопасности
данных.
14. Понятие мониторов безопасности. 4.Физические средства защиты
информации
15. Нормативные руководящие документы в сфере обеспечения ИБ
16. Понятие политики безопасности.
Дискреционные политики безопасности. Мандатные политики безопасности
17. Модель безопасности информационных потоков.
18.Показатели эффективности
систем защиты информации.
19.Способы оценки эффективности систем защиты информации.
20.Руководящие документы Гостехкомиссии в сфере обеспечения ИБ

Вопросы к экзамену по дисциплине «Информационная безопасность»
1.Основные понятия ИБ.
2.Информация,защищаемая информация, ценность информации, уровень секретности.
3.Объекты защиты информации.
4.Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.
5.Классификация угроз безопасности: каналы утечки, воздействия.
6.Прямые и косвенные каналы утечки данных.
7. Основы теории ИБ
8.Модель потенциального нарушителя.
9.Способы мошенничества в информационных системах. 3.Основные способы
реализации угроз ИБ.

10.Основные понятия теории ИБ.
11. Оценка эффективности систем защиты информации
12.Принципы организации систем
обеспечения безопасности данных.
13.Требования, предъявляемые к системам обеспечения безопасности
данных.
14. Понятие мониторов безопасности. 4.Физические средства защиты
информации
15. Нормативные руководящие документы в сфере обеспечения ИБ
16. Понятие политики безопасности.
Дискреционные политики безопасности. Мандатные политики безопасности
17. Модель безопасности информационных потоков.
18.Показатели эффективности
систем защиты информации.
19.Способы оценки эффективности систем защиты информации.
20.Руководящие документы Гостехкомиссии в сфере обеспечения ИБ
21.Программно-технические средства обеспечения ИБ
22.Основные понятия теории ИБ.
23.Принципы организации систем
обеспечения безопасности данных.
24.Требования, предъявляемые к системам обеспечения безопасности данных.
25.Понятие мониторов безопасности.
26.Физические средства защиты информации
27.Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. «Общие критерии». 28.Структура. Основные понятия.
29.Программно-технические средства обеспечения ИБ.
30.Межсетевые экраны.
31.Борьба с компьютерными вирусами
32.Типы компьютерных вирусов.
33.Методы борьбы с компьютерными вирусами.
34. Криптографические методы
35.Федеральный стандарт США на шифрование данных (стандарт DES).
36.Отечественный стандарт шифрование данных.
37. Шифрование с открытым ключом, алгоритм RSA.
38.Построение защищённых виртуальных сетей
39.Понятие, назначение и основные функции защищённой виртуальной сети.
40.Средства построения защищённой виртуальной сети.
41.Туннелирование в протоколах различных уровней.

Тесты для проверки остаточных знаний

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности
2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы
3) Виды информационной безопасности:
+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная
4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций
5) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы
6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации
7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы
8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы
9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей
тест 10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его
16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа
17) ЭЦП – это:
- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор

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» .

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 практического занятия студентам выдаются задания для внеаудиторного выполнения по соответствующей теме;
- срок выполнения задания устанавливается по расписанию занятий (к очередной лекции или практическому 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;
- студентам не получившим зачетное количество баллов по текущему контролю выдается дополнительные задания на зачетном занятии в промежуточную аттестацию.

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.

Основные формы промежуточной аттестации: зачет и 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:

- зачетное занятие (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 зачетном задании;
- 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 экзаменационно-зачетную 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.

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.