Приложение А

(обязательное к рабочей программе дисциплины)

Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Программно-аппаратные средства защиты информации»

Уровень образования **бакалавриат**
(бакалавриат/магистратура/специалитет)

Направление **10.03.01 Информационная безопасность**
(код, наименование специальности)

Профиль **Безопасность автоматизированных систем**
(наименование)

Разработчик _____ Качаева Г.И.
подпись (ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры ИБ «20» сентября 2021г., протокол № 2

Зав. кафедрой _____ Качаева Г.И.
подпись (ФИО уч. степень, уч. звание)

г. Махачкала 2021

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Программно-аппаратные средства защиты информации» 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 10.03.01 Информационная.

Рабочей программой дисциплины «Программно-аппаратные средства защиты информации» предусмотрено формирование следующих компетенций:

ОПК-10 - Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

ОПК-4.3 - Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем

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

Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля), и используемые оценочные средства приведены в таблице 1.

Перечень оценочных средств, рекомендуемых для заполнения таблицы 1 (в ФОС не приводится, используется только для заполнения таблицы)

- *Тест (для текущего контроля)*
- *Устный опрос*
- *Эссе*
- *Вопросы для проведения экзамена*

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

Таблица 1

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	Критерии оценивания	Наименование контролируемых разделов и тем[1]
ОПК-10 - Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1.1 - знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	№№1-34
	ОПК-10.2.1 - умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	№№1-34
ОПК-4.3 - Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе	ОПК-4.3.1. Знает принципы устройства и функционирования программных, программно-аппаратных и технических средств защиты информации.	Знает принципы устройства и функционирования программных, программно-аппаратных и технических средств защиты информации.	№№1-34
	ОПК-4.3.1. Умеет использовать программные, программно-аппаратные (в том числе криптографические) и технические	Умеет использовать программные, программно-аппаратные (в том числе криптографические) и технические средства для защиты информации в автоматизированных системах.	№№1-34

[1] *Наименования разделов и тем должен соответствовать рабочей программе дисциплины.*

криптографических) и технических средств защиты информации автоматизированных систем	средства для защиты информации в автоматизированных системах.		
	ОПК-4.3.1. Владеет методами установки и настройки программных, программно-аппаратных и технических средств защиты информации.	Владеет методами установки и настройки программных, программно-аппаратных и технических средств защиты информации.	№№1-34

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине Программно-аппаратные средства защиты информации определяется на следующих этапах:

1. **Этап текущих аттестаций** *(Для проведения текущих аттестаций могут быть использованы оценочные средства, указанные в разделе 2)*

2. **Этап промежуточных аттестаций** (*Для проведения промежуточной аттестации могут быть использованы другие оценочные средства*)

Таблица 2

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	**Этапы формирования компетенции**					
		Этап текущих аттестаций					**Этап промежуточной аттестации**
		1-5 неделя	**6-10 неделя**	**11-15 неделя**	**1-17 неделя**		**18-20 неделя**
		Текущая аттестация №1	Текущая аттестация №2	Текущая аттестация №3	СРС	КР/КП	Промежуточная аттестация
1		**2**	**3**	**4**	**5**	**6**	**7**
ОПК-10- Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1.1 - знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ОПК-10.2.1 - умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена

	политиками безопасности						
ОПК-4.3- Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1. Знает принципы устройства и функционирования программных, программно-аппаратных и технических средств защиты информации.	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ОПК-4.3.1. Умеет использовать программные, программно-аппаратные (в том числе криптографические) и технические средства для защиты информации в автоматизированных системах.	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ОПК-4.3.1. Владеет методами установки и настройки программных, программно-аппаратных и технических средств защиты информации.	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена

СРС – самостоятельная работа студентов;
КР – курсовая работа;
КП – курсовой проект.

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 Программно-аппаратные средства защиты информации 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 основных понятий 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 обладает необходимыми знаниями для их устранения.	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения практическими умениями и навыками,

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
	Обучающимся продемонстрирован базовый уровень освоения компетенции	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.

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

3.1. Задания и вопросы для входного контроля

1. Формальное описание структуры информационной системы.
2. Составление модели угроз информационной системе.
3. Формирование требований к системе защиты информации.
4. Формирование требований к политике информационной безопасности.
5. Формирование регламента действий при возникновении нештатных ситуаций.

3.2. Задания для промежуточной аттестации

3.2.1. Тест (для текущего контроля)

Указания:
Задания имеют разное количество вариантов ответа, из которых правильными могут быть как один, так и несколько вариантов. В листе ответа проставляются номера правильных ответов.

1. Сколько уровней возможностей нарушителей предоставляемых им штатными средствами КС предусмотрено классификацией в соответствии с РД ГТК (ФСТЭК)?

a) Один.
b) Два.
c) Три.
d) Четыре.
e) Пять.
f) Семь.

2. Схемы разграничения доступа в которых защитные механизмы встраиваются в каждый объект и осуществляют контроль в соответствии со отеками доступа данного объекта называются:

a) «Списковые» схемы (дискреционный доступ).
b) «Мандатные» схемы (мандатный доступ).
c) «Полномочные» схемы (полномочный доступ).

3. Документ «Служба директорий: обзор концепций, моделей и сервисов» относится к:

a) 1 Оценочным стандартам
b) 2 Техническим спецификациям
c) 3 Руководящим документам ФСТЭК

4. В каком году был принят Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Trusted Computer System Evaliation Criteria, TCSEC)?

a) 1 1975
b) 2 1980
c) 3 1985
d) 4 1990

5. Каким стандартом было введено понятие: «Сетевая доверенная вычислительная база»?

a) 1 Department of Defense Trusted Computer System Evaliation Criteria, TCSEC
b) 2 Trusted Network Interpretation
c) 3 ISO/IEC 15408-99
d) 4 ГОСТ/ИСО МЭК 15408:2002

6. Какой стандарт называют «Оранжевой книгой»?

a) 1 Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Department of Defense Trusted Computer System Evaliation Criteria, TCSEC)
b) 2 Гармонизированные критерии Европейских стран" [европейские критерии]
c) 3 Международный стандарт ISO/IEC 15408-99 «Критерии оценки безопасности информационных технологий» (Evaluation criteria for IT security)

7. Какой стандарт сокращенно называют «Общими критериями» (ОК)?

a) 1 Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем»
b) 2 Международный стандарт ISO/IEC 15408-99
c) 3 Британский стандарт BS 7799 «Управление информационной безопасностью. Практические правила»

8. Какое из перечисленных понятий было введено в Стандарте Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Trusted Computer System Evaliation Criteria, TCSEC)?

a) 1 Сервисы безопасности
b) 2 Политика безопасности
c) 3 Оценочные уровни доверия - ОУД

9. Международный стандарта ISO/IEC 15408-99 раскрывает (описывает):
Систематический подход к вопросам доступности, формирование архитектурных принципов ее обеспечения.

a) Различие между системами и продуктами информационных технологий, но для унификации требований вводится единое понятие - объект оценки
b) Критерии оценки безопасности информационных технологий

10. Как называется документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг?

a) 1 Технические условия
b) 2 Спецификация
c) 3 Регламент
d) 4 Стандарт

11. Цель создания политики информационной безопасности?

a) Для организационно-технической поддержки политики формирования и использования информационных ресурсов при осуществлении доступа к информации
b) Для защиты от внешних деструктивных воздействий
c) Для защиты от недобросовестных работников (пользователей)

12. Совокупность принципов, правил и рекомендаций, определяющих порядок организации защиты информации, обрабатываемой в конкретной компьютерной системе, зафиксированная документально называется:

a) 1 Технической политикой безопасности компьютерной системы
b) 2 Политикой информационной безопасности компьютерной системы
c) 3 Стандарт безопасности компьютерной системы

13. Формулировка целей, которые преследует организация в области безопасности информации, определение общих направлений в достижении этих целей является составной частью:

a) 1 Политики безопасности верхнего (правового и административного) уровня
b) 2 Политики безопасности среднего (процедурного) уровня
c) 3 Политики безопасности нижнего (программно-аппаратного) уровня
d) 4 Нет правильного ответа

14. Контроль участников взаимодействия является ключевым моментом при составлении политики информационной безопасности:

a) 1 Политики безопасности верхнего (правового и административного) уровня
b) 2 Политики безопасности среднего (процедурного) уровня
c) 3 Политики безопасности нижнего (программно-аппаратного) уровня
d) 4 Нет правильного ответа

15. Список подчиненных политик безопасности является основой:

a) Acceptable use policies - AUP
b) Корневой политики безопасности
c) Политики формирования и использования информационных ресурсов

16. Совокупность требований и правил по информационной безопасности для объекта информационной безопасности, выработанных в соответствии с требованиями руководящих и нормативных документов в целях противодействия заданному множеству угроз информационной безопасности, с учетом ценности защищаемой информационной сферы и стоимости системы обеспечения информационной безопасности называется:

a) 1 Стандарт безопасности
b) 2 Политика информационной безопасности
c) 3 Политика безопасности верхнего уровня
d) 4 Корневая политика безопасности

17. В каком документе (разделе) политики безопасности отражается ответ на вопрос:

a) «Существуют ли ограничения на установку ПО»?
b) 1 Сертификате безопасности
c) 2 Acceptable use policies - AUPS
d) 3 Incident response plan - IRP
e) 4 Password policy

18. Какой документ включает в себя следующие подразделы: политику формирования и использования информационных ресурсов, политику информационной безопасности и техническую политику?

a) Стандарт безопасности
b) Техническая спецификация
c) Информационная политика
d) Политика информационной безопасности
e) Политика использования информационных ресурсов

19. В политике безопасности какого уровня описывается отношение к передовым, но еще недостаточно проверенным технологиям защиты информации?

a) 1 Правового и административного
b) 2 Процедурного
c) 3 Аппаратно-программного

20. Что определяет системная информационная политика?

a) 1 Принципы, порядок и правила интеграции информационных ресурсов
b) 2 Принципы, порядок и правила построения систем защиты информации
c) 3 Принципы, порядок и правила разграничения доступа к информационным ресурсам

21. Как называется внешняя или внутренняя по отношению к атакуемой компьютерной системе программа, обладающая определенными деструктивными функциями по отношению к этой системе?

a) 1 Компьютерный вирус
b) 2 Программная закладка
c) 3 Аппаратная закладка

22. Как называется несаморазмножающаяся программа, обеспечивающая злоумышленнику возможности несанкционированного доступа к защищаемой информации?

a) 1 Компьютерный вирус
b) 2 Ловушка
c) 3 Люк
d) 4 Логическая бомба

23. Какая из перечисленных функций не относится к программным закладкам?

a) 1 Уничтожение информации
b) 2 Самостоятельное распространение в компьютерных системах
c) 3 Перехват и передача информации
d) 4 Целенаправленная модификация кода программы

24. По какому признаку классифицируются «драйверные закладки»?

a) 1 По методу внедрения
b) 2 По принципу действия
c) 3 По деструктивным последствиям

25. Какое из перечисленных воздействий не относится к моделям воздействия программных закладок?

a) 1 Уборка мусора
b) 2 Искажение
c) 3 Наблюдение
d) 4 Копирование
e) 5 Перехват

26. К какому виду РПС относится «Клавиатурный шпион»

a) 1 К программным закладкам
b) 2 К вирусам
c) 3 К бактериям

27. Какие из перечисленных свойств присущи компьютерным вирусам?

a) 1 Способность к включению своего кода в тела других файлов и системных областей
b) памяти компьютера
c) Способность к последующему самостоятельному выполнению и самовоспроизведению
d) 3 Способность к самостоятельному распространению в КС
e) 4 Все перечисленные свойства
f) 5 Только 1 и 3 свойство
g) 6 Только 2 и 3 свойство

28. Сотрудник Лехайского университета (США) Фред Коэн:

a) 1 Впервые создал антивирус
b) 2 Сделал сообщение о возможности существования компьютерных вирусов
c) 3 Является создателем вируса-червя

29. В чем принципиальное отличие компьютерного вируса от программной закладки?

a) 1 Сложностью написания
b) 2 Возможностью деструктивного воздействия
c) 3 Способностью к саморазмножению и модификации
d) 4 Всеми вышеперечисленными свойствами

30. Как называются закладки, интерфейс которых, совпадает с интерфейсом некоторых служебных программ, требующих ввод конфиденциальной информации

a) 1 Прикладные закладки
b) 2 Исполняемые закладки
c) 3 Закладки-имитаторы
d) 4 Закладки-невидимки

31. По какому признаку вирус классифицируется как резидентный вирус?

a) 1 По режиму функционирования
b) 2 По объекту внедрения
c) 3 По особенностям реализуемого алгоритма
d) 4 По деструктивным возможностям

32. По какому признаку вирус классифицируется как «stealth-вирус»?

a) 1 По объекту внедрения
b) 2 По особенностям реализуемого алгоритма
c) 3 По деструктивным возможностям

33. По какому признаку вирус классифицируется как «загрузочный (бутовый) вирус»?

a) 1 По объекту внедрения
b) 2 По особенностям реализуемого алгоритма
c) 3 По режиму функционирования

34. Вирусы, содержащие в себе алгоритмы шифрования и обеспечивающие различие разных копий вируса называются:

a) 1 Вирусы-спутники
b) 2 Stealth-вирусы
c) 3 MtE-вирусы
d) 4 Репликаторы

35. К какому типу компьютерных вирусов относятся полиморфные вирусы?

a) 1 К MtE-вирусам
b) 2 К Stealth-вирусам
c) 3 К вирусам-спутникам

36. 31 По какому признаку компьютерный вирус классифицируется как репликатор?
a) 1 По особенностям реализуемого алгоритма
b) 2 По объекту внедрения
c) 3 По наличию дополнительных возможностей

37. Вирусы, создающие для заражаемых файлов одноименные файлы с кодом вируса и переименовывающие исходные файлы называются:
a) 1 Вирусы - спутники
b) 2 Вирусы - невидимки
c) 3 Вирусы - мутанты

38. Как называется компьютерный вирус, который использует слабую защищенность некоторых ОС и заменяет некоторые их компоненты (драйверы дисков, прерывания)?
a) 1 Файловым
b) 2 Загрузочным
c) 3 Stealth-вирус
d) 4 Репликатор

39. Как называются группы из нескольких вирусов?
a) 1 Поливирусами
b) 2 Семейством вирусов
c) 3 Вирусным классом
d) 4 Нет верных ответов

40. Какие вирусы характеризуются способностью самостоятельно передавать свой код на удаленный сервер или рабочую станцию?
a) 1 Файловые вирусы
b) 2 Бутовые (загрузочные) вирусы
c) 3 Нет правильных ответов
d) 4 Файловых и загрузочных вирусы

3.2.2. Аттестационная контрольная работа №1

1. Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации.
2. Каналы утечки речевой информации.
3. Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники.
4. Индикаторы электромагнитных излучений.
5. Радиочастотомеры.
6. Нелинейные локаторы.
7. Досмотровая техника
8. Организационно-методические основы защиты информации.
9. Общие требования к защите информации.
10. Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации.

3.2.3. Аттестационная контрольная работа №2

11. Организация защиты информации от утечки возникающей при работе вычислительной техники за счет ПЭМИН.
12. Методология защиты информации от утечки за счет ПЭМИН.
13. Критерий защищенности средств вычислительной техники.
14. Нормированные уровни помех в каналах утечки.
15. Методика проведения специальных исследований технических средств ЭВТ.

3.2.4. Аттестационная контрольная работа №3

1. Специальные проверки.
2. Порядок проведения специальной проверки технических средств
3. Специальные обследования.
4. Подготовка к проведению специальных обследований.
5. Выполнение поисковых мероприятий.
6. Подготовка отчетных материалов.
7. Категории программных ошибок.
8. Типы тестов. Тестирование на этапе планирования.
9. Тестирование на этапе проектирования.
10. Тестирование "белого ящика" на стадии кодирования.
11. Регрессионное тестирование. Тестирование "черного ящика".
12. Разработка тестов.

3.2.5. Эссе

1. Основные понятия и определения в области защиты компьютерной информации.
2. Современная ситуация в области защиты компьютерной информации.
3. Требования к системам защиты информации.
4. Понятие угрозы безопасности компьютерной информации. Интервал потенциальной опасности.
5. Классификация угроз безопасности компьютерной информации.
6. Источники, риски и формы атак на информацию.
7. Принципы защиты компьютерной информации
8. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация; 9 Основные подходы к защите данных от НСД (контроль доступа и разграничение доступа, иерархический доступ к файлу).
9. Формальные модели управления доступом.
10. Классификация средств защиты компьютерной информации от НСД
11. Аутентификация пользователей. Основные алгоритмы (протоколы) аутентификации.
12. Администрирование сетей в аспекте безопасности информации
13. Защита сетевого файлового ресурса, фиксация доступа к файлам.
14. Доступ к данным со стороны процесса, способы фиксации факта доступа.
15. Надежность систем ограничения доступа;
16. Защита файлов от изменения;
17. Электронная цифровая подпись (ЭЦП);
18. Методы и средства ограничения доступа к компонентам ЭВМ;
19. Программно-аппаратные средства шифрования;
20. Построение аппаратных компонент криптозащиты данных;
21. Защита алгоритма шифрования.
22. Принцип чувствительной области и принцип главного ключа,
23. Пароли и ключи, организация хранения ключей;
24. Необходимые и достаточные функции аппаратного средства криптозащиты;
25. Защита программ от несанкционированного копирования;
26. Защита программ от изучения;
27. Защита программ от отладки, защита от дизассемблирования,
28. Защита программ от трассировки по прерываниям;
29. Защита от разрушающих программных воздействий (РПВ);
30. Компьютерные вирусы как особый класс РПВ;
31. Необходимые и достаточные условия недопущения разрушающего воздействия; Понятие изолированной программной среды.
32. Общая характеристика и классификация вредоносных программ.
33. Компьютерные вирусы. Классификация компьютерных вирусов.

34. Основы технологии анализа защищенности компьютерных систем управления и обработки информации.
35. Многоуровневая защита корпоративных сетей.

3.2.6. Список вопросов к экзамену

1. Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации.
2. Каналы утечки речевой информации.
3. Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники.
4. Индикаторы электромагнитных излучений.
5. Радиочастотомеры.
6. Нелинейные локаторы.
7. Досмотровая техника
8. Организационно-методические основы защиты информации.
9. Общие требования к защите информации.
10. Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации
11. Организация защиты информации от утечки возникающей при работе вычислительной техники за счет ПЭМИН.
12. Методология защиты информации от утечки за счет ПЭМИН.
13. Критерий защищенности средств вычислительной техники.
14. Нормированные уровни помех в каналах утечки.
15. Методика проведения специальных исследований технических средств ЭВТ.
16. Специальные проверки.
17. Порядок проведения специальной проверки технических средств
18. Специальные обследования.
19. Подготовка к проведению специальных обследований.
20. Основные направления, методы и средства технического противодействия закладным устройствам.
21. Оптико-электронный канал утечки речевой информации. Лазерные микрофоны интерферометрического и дифференциально-интерферометрического принципов действия.
22. Понятие о демаскирующих признаках объекта. Демаскирующие признаки сигналов.
23. Механизм (методика, принцип) обнаружения и классификации опасных сигналов.
24. Методы локализации закладных устройств. Метод энергетического зондирования. Метод акустической и радиолокационной триангуляции.
25. Атрибуты и признаки потенциально опасного сигнала закладных устройств.
26. Государственная система (иерархия) в области технических средств защиты информации. Основные руководящие, нормативные и методические документы.
27. Технический контроль эффективности мер по защите информации. Общая методика проведения технического контроля (ПЭМИН, акустических и виброакустических каналов утечки).

Зачеты и экзамены могут быть проведены в письменной форме, а также в письменной форме с устным дополнением ответа. Зачеты служат формой проверки качества выполнения студентами лабораторных работ, усвоения семестрового учебного материала по дисциплине (модулю), практических и семинарских занятий (при отсутствии экзамена по дисциплине).

По итогам зачета, соответствии с модульно – рейтинговой системой университета, выставляются баллы с последующим переходом по шкале баллы – оценки за зачет, выставляемый как по наименованию «зачтено», «не зачтено», так и дифференцированно т.е. с выставлением отметки по схеме – «отлично», «хорошо», «удовлетворительно» и

«неудовлетворительно», определяемое решением Ученого совета университета и прописываемого в учебном плане.

Экзамен по дисциплине (модулю) служит для оценки работы студента в течении семестра (года, всего срока обучения и др.) и призван выявить уровень, качество и систематичность полученных им теоретических и практических знаний, приобретения навыков самостоятельной работы, развития творческого мышления, умения синтезировать полученные знания и применять их в решении практических задач. По итогам экзамена, в соответствии с модульно – рейтинговой системой университета выставляются баллы, с последующим переходом по шкале оценок на оценки: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», свидетельствующие о приобретенных компетенциях или их отсутствии.

Форма экзаменационного билета (пример оформления)

Министерство науки и высшего образования РФ

ФГБОУ ВО "Дагестанский государственный технический университет"

Дисциплина (модуль) Программно-аппаратные средства защиты информации
Код, направление 10.03.01 Информационная безопасность
профиль Безопасность автоматизированных систем
Кафедра ИБ Курс 3 Семестр 6
Форма обучения – очная

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1.

1. Порядок проведения специальной проверки технических средств
2. Каналы утечки речевой информации.

Экзаменатор……Качаева Г.И.

Утвержден на заседании кафедры (протокол №___ от _____20___ г.)

Зав. кафедрой (название) ……...Качаева Г.И.

В ФОС размещается пример заполненного экзаменационного билета. Весь комплект экзаменационных билетов по дисциплине хранится на кафедре в соответствии с утвержденной номенклатурой дел.

Критерии оценки уровня сформированности компетенций по результатам проведения зачета:

- оценка «зачтено»: обучающийся демонстрирует всестороннее, систематическое и глубокое знание материала, свободно выполняет задания, предусмотренные программой дисциплины, усвоивший основную и дополнительную литературу. Обучающийся выполняет задания, предусмотренные программой дисциплины, на уровне не ниже базового;
- оценка «не зачтено»: обучающийся демонстрирует незнание материала, не выполняет задания, предусмотренные программой дисциплины. Обучающийся не выполняет задания, предусмотренные программой дисциплины, на уровне ниже базового. Дальнейшее освоение ОПОП не возможно без дополнительного изучения материала и подготовки к зачету.

Критерии оценки уровня сформированности компетенций по результатам проведения дифференцированного зачёта (зачета с оценкой) / экзамена:

- оценка **«отлично»:** обучающийся дал полный, развернутый ответ на поставленный вопрос, проявил совокупность осознанных знаний об объекте, доказательно раскрыл основные положения темы. В ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, явлений. Обучающийся подкрепляет теоретический ответ практическими примерами. Ответ сформулирован научным языком, обоснована авторская позиция обучающегося. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа или с помощью «наводящих» вопросов преподавателя. Обучающимся продемонстрирован высокий уровень владения компетенцией(-ями);

- оценка **«хорошо»:** обучающимся дан полный, развернутый ответ на поставленный вопрос, проявлено умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, но есть недочеты в формулировании понятий, решении задач. При ответах на дополнительные вопросы допущены незначительные ошибки. Обучающимся продемонстрирован повышенный уровень владения компетенцией(-ями);

- оценка **«удовлетворительно»:** обучающимся дан неполный ответ на вопрос, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, явлений, нарушена логика ответа, не сделаны выводы. Речевое оформление требует коррекции. Обучающийся испытывает затруднение при ответе на дополнительные вопросы. Обучающимся продемонстрирован базовый уровень владения компетенцией(-ями);

- оценки **«неудовлетворительно»:** обучающийся испытывает значительные трудности в ответе на вопрос, допускает существенные ошибки, не владеет терминологией, не знает основных понятий, не может ответить на «наводящие» вопросы преподавателя. Обучающимся продемонстрирован низкий уровень владения компетенцией(-ями).