ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»

Утвержден решением
Ученого совета ДГУНХ,
протокол № 11
от 24 марта 2025 г

КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО МЕЖДИСЦИПЛИНАРНОМУ КУРСУ «ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация – техник по защите информации

Форма обучения – очная

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A9E2DAF91A2F57E988B751E574CFCC
Владелец: Бучаев Ахмед Гамидович
Действителен: с 23.09.2025 до 17.12.2026

Махачкала – 2025

УДК 681.518(075.8)

ББК 32.81.73

Составитель – Эмирбеков Эльдар Меликович, старший преподаватель кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры "Математические методы в экономике" Дагестанского государственного университета.

Представитель работодателя - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза».

*Фонд оценочных средств по междисциплинарному курсу «*Программно-аппаратные средства защиты информации*» разработаны в соответствии с требованиями федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённого приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г., № 1553, в соответствии с приказом Минпросвещения России от 24.08.2022 г., № 762 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования».*

Фонд оценочных средств по междисциплинарному курсу «Программно-аппаратные средства защиты информации» размещены на официальном сайте www.dgunh.ru

Эмирбеков Э.М. Фонд оценочных средств по междисциплинарному курсу «Программно-аппаратные средства защиты информации» для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. – Махачкала: ДГУНХ, 2025 г. – 46 с.

Рекомендован к утверждению Учебно-методическим советом ДГУНХ 10 марта 2025 г.

Рекомендован к утверждению руководителем образовательной программы СПО – программы подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, к.пед.н., Гасановой З.А.

Одобрен на заседании кафедры «Информационные технологии и информационная безопасность» 24 февраля 2025 г., протокол № 7.

СОДЕРЖАНИЕ

Назначение оценочных материалов

Фонд оценочных средств для текущего контроля успеваемости (оценивания хода освоения дисциплин), для проведения промежуточной аттестации (оценивания промежуточных и окончательных результатов обучения по междисциплинарному курсу) обучающихся по междисциплинарному курсу «Программно-аппаратные средства защиты информации» на соответствие их учебных достижений поэтапным требованиям образовательной программы 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Фонд оценочных средств по междисциплинарному курсу «Программно-аппаратные средства защиты информации» включают в себя: перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины; описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания; типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения ОПОП; методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Фонд оценочных средств сформированы на основе ключевых принципов оценивания:

- валидности: объекты оценки должны соответствовать поставленным целям обучения;

- надежности: использование единообразных стандартов и критериев для оценивания достижений;

- объективности: разные обучающиеся должны иметь равные возможности для достижения успеха.

Основными параметрами и свойствами оценочных материалов являются:

- предметная направленность (соответствие предмету изучения конкретной дисциплины);

- содержание (состав и взаимосвязь структурных единиц, образующих содержание теоретической и практической составляющих дисциплины);

- объем (количественный состав оценочных материалов);

- качество оценочных материалов в целом, обеспечивающее получение объективных и достоверных результатов при проведении контроля с различными целями.

-

РАЗДЕЛ 1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ВИДОВ ОЦЕНОЧНЫХ СРЕДСТВ В ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Перечень формируемых компетенций

код компетенции	формулировка компетенции
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

1.2. Перечень компетенций с указанием видов оценочных средств

Формируемые компетенции	***Планируемые результаты обучения по междисциплинарному курсу, характеризующие этапы формирования компетенций***	***Уровни освоения компетенций***	***Критерии оценивания сформированности компетенций***	***Виды оценочных средств***
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации ПК	**Знать:** – виды и назначение программно-аппаратных средств защиты информации	Пороговый уровень	Обучающийся слабо (частично) знает – виды и назначение программно-аппаратных средств защиты информации	**Блок А –**задания репродуктивного уровня – вопросы для обсуждения - тестирование
		Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает – виды и назначение программно-аппаратных средств защиты информации	
		Продв	Обучающийся с	

		инутый уровень	требуемой степенью полноты и точности знает – виды и назначение программно-аппаратных средств защиты информации	
	Уметь: - грамотно использовать аппаратные средства защиты при решении практических задач	Пороговый уровень	Обучающийся слабо (частично) умеет грамотно использовать аппаратные средства защиты при решении практических задач	**Блок В** – задания реконструктивного уровня – Лабораторные работы; - тестирование
		Базовый уровень	Обучающийся с незначительными затруднениями умеет грамотно использовать аппаратные средства защиты при решении практических задач	
		Продвинутый уровень	Обучающийся умеет грамотно использовать аппаратные средства защиты при решении практических задач	
	Владеть: - применения наиболее эффективных методов и средств программно-аппаратной защиты информации	Пороговый уровень	Обучающийся слабо (частично) владеет применения наиболее эффективных методов и средств программно-аппаратной защиты информации	**Блок С** – задания практико-ориентированного уровня Лабораторные работы - тестирование
		Базовый уровень	Обучающийся с небольшими затруднениями применения наиболее эффективных методов и средств программно-аппаратной защиты информации	
		Продвинутый уровень	Обучающийся свободно владеет применения наиболее эффективных методов и средств программно-аппаратной защиты информации	
2.2.Обеспечивать защиту информации в автоматизированных	**Знать:** – способы проведения проверки работоспособности и эффективности	Пороговый уровень	Обучающийся слабо (частично) знает – способы проведения проверки работоспособности и эффективности	**Блок А –**задания репродуктивного уровня – вопросы для обсуждения

системах отдельными программными, программно-аппаратными средствами. ПК 2.3.Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации ПК 2.5.Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств ПК 2.6.Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств	применяемых программно-аппаратных средств защиты информации		применяемых программно-аппаратных средств защиты информации	- тестирование
		Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает – способы проведения проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	
		Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает – способы проведения проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	
	Уметь: – осуществлять проверку работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	Пороговый уровень	Обучающийся слабо (частично) знает – осуществлять проверку работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	**Блок В** – задания реконструктивного уровня – Лабораторные работы; - тестирование
		Базовый уровень	Обучающийся с незначительными затруднениями умеет осуществлять проверку работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	
		Продвинутый уровень	Обучающийся умеет осуществлять проверку работоспособности и эффективности применяемых	

обнаружения, предупреждения и ликвидации последствий компьютерных атак			программных, программно-аппаратных средств защиты	
	Владеть: – навыками проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	Пороговый уровень	Обучающийся слабо (частично) владеет – навыками проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	
		Базовый уровень	Обучающийся с небольшими затруднениями – навыками проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	**Блок С** – задания практико-ориентированного уровня Лабораторные работы - тестирование
		Продвинутый уровень	Обучающийся свободно владеет – навыками проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	

РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по междисциплинарному курсу

Для проверки сформированности компетенции
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
репродуктивного уровня («знать»)

.

Блок А. Задания репродуктивного уровня («знать»)

А1. Тестовые задания

1. Прочтите текст задания и выберите один верный ответ

При установке антивирусного ПО, какой параметр обязательно нужно настроить для обеспечения актуальной защиты?

Варианты ответов:

а. Интервал сканирования системы
б. Включение режима «Игровой режим»
в. Автоматическое обновление вирусных баз
г. Отключение сканирования архивов

2. Прочтите текст задания и выберите один верный ответ

При настройке межсетевого экрана (брандмауэра) для сервера, что нужно сделать в первую очередь?

Варианты ответов:

а. Разрешить все входящие соединения
б. Запретить весь входящий трафик и добавить правила разрешения только для необходимых портов и IP
в. Отключить брандмауэр для тестирования
г. Разрешить исходящий трафик без ограничений

3. Прочтите текст задания и выберите один верный ответ

Что является обязательным шагом при установке средства шифрования диска (например, BitLocker или VeraCrypt)?

Варианты ответов:

а. Форматирование диска
б. Создание и безопасное хранение ключа восстановления
в. Отключение шифрования системного раздела
г. Установка пароля пользователя

4. Прочтите текст задания и выберите один верный ответ

При установке системы обнаружения вторжений (IDS), где рекомендуется разместить сенсор для сетевого мониторинга?

Варианты ответов:

а. На рабочем компьютере пользователя
б. В точке, где сенсор может «видеть» весь сетевой трафик (SPAN-порт коммутатора)
в. На сервере базы данных
г. За маршрутизатором

5. Прочтите текст задания и выберите один верный ответ

При настройке двухфакторной аутентификации (2FA) с использованием аппаратного токена, что нужно сделать перед выдачей токена пользователю?

Варианты ответов:

а. Установить ПО на токен
б. Произвести синхронизацию токена с сервером аутентификации
в. Зарегистрировать токен в антивирусе
г. Настроить брандмауэр

6. Прочтите текст задания и выберите один верный ответ

Что НЕ рекомендуется делать при установке программного средства контроля целостности (File Integrity Monitoring — FIM)?

Варианты ответов:

а. Выбрать критичные файлы и реестровые ключи для мониторинга
б. Настроить оповещение при изменениях
в. Отключать мониторинг после настройки
г. Указать путь к журналу событий

7. Прочтите текст задания и выберите один верный ответ

При установке системы предотвращения вторжений (IPS), какой тип правил нужно обязательно активировать?

Варианты ответов:

а. Правила для разрешения веб-трафика
б. Правила для блокировки известных сигнатур атак
в. Правила резервного копирования
г. Правила автоматического обновления ОС

8. Прочтите текст задания и выберите один верный ответ

Что нужно проверить сразу после установки любого средства защиты?

Варианты ответов:

а. Свободное место на диске
б. Функционирование средства и отсутствие конфликтов с другими программами
в. Скорость интернета
г. Дизайн интерфейса

9. Прочтите текст задания и выберите один верный ответ

При настройке политики паролей через групповые политики (GPO), какой параметр наиболее важен для безопасности?
Варианты ответов:

а. Минимальная длина пароля — 12 символов
б. Требование использования заглавных букв
в. Срок действия пароля — 90 дней
г. Хранение паролей в открытом виде

10. Прочтите текст задания и выберите один верный ответ

Для установки аппаратного средства защиты (например, аппаратного брандмауэра), что является первым шагом?
Варианты ответов:

а. Подключение к электросети
б. Физическое подключение к сети в соответствии с топологией
в. Установка ПО управления
г. Настройка IP-адреса

А2. Вопросы для обсуждения

1. Виды и источники угроз информационной безопасности РФ.
2. Классификация программно-аппаратных средств защиты информации
3. Структура государственной системы обеспечения информационной безопасности РФ.
4. Правовое регулирование информационной сферы в РФ.
5. Основные нормативно-методические материалы.
6. Понятия: информация, информатизация, информационные технологии, информационные ресурсы.
7. Понятие программно-аппаратной защиты информации.
8. Задачи программно-аппаратной защиты информации.
9. Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тестовые задания

Прочтите текст и установите последовательность

Упорядочите последовательность этапов установки программного средства защиты информации:
Варианты ответов:

а. Проверка совместимости с операционной системой
б. Загрузка дистрибутива

в. Запуск инсталлятора
г. Конфигурация параметров безопасности
д. Перезагрузка системы

Прочтите текст и установите последовательность
Упорядочите этапы первоначальной настройки программно-аппаратного комплекса защиты:
Варианты ответов:
а. Документирование параметров5
б. Инициализация аппаратного модуля1
в. Тестирование функциональности4
г. Установка программного обеспечения2
д. Загрузка сертификатов3

Прочтите текст и установите последовательность
Упорядочите последовательность настройки политик безопасности:
Варианты ответов:
а. Документирование установленных политик
б. Определение требований безопасности
в. Создание профилей доступа
г. Применение политик к пользователям
д. Проверка соответствия требованиям

Прочтите текст и установите последовательность
Упорядочите процесс инсталляции межсетевого экрана:
Варианты ответов:
а. Мониторинг работоспособности
б. Установка программного обеспечения
в. Активация защиты
г. Конфигурация правил фильтрации
д. Подключение к сетевым интерфейсам

Прочтите текст и установите последовательность
Упорядочите этапы конфигурации системы шифрования данных:
Варианты ответов:
а. Выбор алгоритма шифрования1
б. Проверка корректности шифрования5
в. Генерация ключей2
г. Сохранение резервной копии ключей4
д. Применение к защищаемым данным3

В2. Лабораторная работа

Практико-ориентированная лабораторная работа: «Механизмы защиты»

Задание для работы:
1. Список контроля доступа
Краткое описание:
1. Функциональное построение СЗИ организации и назначение основных подразделений.
2. Элементарные модели СЗИ организации. Семирубежная модель защиты.
Результаты и выводы: В ходе работы, студент научился разбираться и оперировать основными понятиями информационной безопасности.

Тема: «Нормативно-методическое обеспечение создания АС**»** 37
Цель работы: исследование состава аппаратных и программных средств персонального компьютера (ПК), составляющих основу его конфигурации
Задание для работы:
1. Нормативно-методическое обеспечение АС.
2. Международные стандарты.
3. Стандарты Российской Федерации.

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

В1. Тестовые задания

Прочтите текст и вставьте пропущенное слово.
Для предотвращения загрузки несанкционированной операционной системы со съемных носителей, при настройке аппаратной части СЗИ необходимо установить пароль на изменения в _____.

Прочтите текст и вставьте пропущенное слово.
Процесс установки большинства программных средств защиты информации в современных ОС требует наличия прав _____ для корректной интеграции драйверов защиты в ядро системы.

Прочтите текст и вставьте пропущенное слово.
Конфигурирование прав доступа в СЗИ, основанное на ролях пользователей, называется _____ моделью управления доступом.

С2. Лабораторная работа

1. Идентификация, аутентификация и авторизация субъектов и объектов системы
Краткое описание:

1. Последовательность и содержание основных этапов проектирования СЗИ организации.
2. Содержание процесса эксплуатации СЗИ организации.

Результаты и выводы: В ходе работы, студент научился разбираться и оперировать основными понятиями информационной безопасности.

Для проверки сформированности компетенции
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами
Блок А. Задания репродуктивного уровня («знать»)

А1 Тестовые задания

1. Прочтите текст задания и выберите один верный ответ

Какое средство используется для разграничения доступа пользователей к ресурсам АС?

Варианты ответов:

а. Антивирус
б. Система управления доступом (например, RBAC — Role-Based Access Control)
в. Система резервного копирования
г. Межсетевой экран

2. Прочтите текст задания и выберите один верный ответ

Для защиты конфиденциальных данных при передаче по сети в АС следует использовать:

Варианты ответов:

а. Антиспам-фильтр
б. Протоколы шифрования (TLS/SSL, IPsec)
в. Систему контроля целостности
г. Резервное копирование

3. Прочтите текст задания и выберите один верный ответ

Что из перечисленного относится к программно-аппаратным средствам защиты в АС?

Варианты ответов:

а. Инструкция по работе пользователя
б. Аппаратный ключ аутентификации (токен)
в. Политика паролей
г. Журнал регистрации событий

4. Прочтите текст задания и выберите один верный ответ

Для предотвращения утечки информации через съемные носители в АС нужно:

Варианты ответов:

а. Разрешить запись на все устройства
б. Запретить использование съемных носителей через групповые политики и использовать шифрование дисков
в. Установить антивирус
г. Разрешить подключение только мыши

4. Прочтите текст задания и выберите один верный ответ

Какое средство автоматически выявляет подозрительную активность в АС?

Варианты ответов:

а. Система резервного копирования
б. Средство шифрования
в. Система обнаружения вторжений (IDS)
г. Антиспам-фильтр

5. Прочтите текст задания и выберите один верный ответ

Для защиты серверов АС от несанкционированного доступа из интернета используется:

Варианты ответов:

a) Антивирус
b) Межсетевой экран (Firewall) с настроенными правилами
c) Система контроля целостности
d) Резервное копирование

7. Прочтите текст задания и выберите один верный ответ

Что позволяет обеспечить целостность критичных файлов в АС?

Варианты ответов:

а. Антивирус
б. Шифрование
в. Средство контроля целостности (File Integrity Monitoring — FIM)
г. Система резервного копирования

8. Прочтите текст задания и выберите один верный ответ

Для централизованного мониторинга и анализа событий безопасности в АС применяется:

Варианты ответов:

а. Антивирус
б. Средство шифрования
в. SIEM-система (Security Information and Event Management)
г. Система резервного копирования

9. Прочтите текст задания и выберите один верный ответ

Защита от атак типа «Brute Force» (подбор пароля) обеспечивается:

Варианты ответов:

а. Антивирусом
б. Системой блокировки учетной записи после нескольких неудачных попыток входа
в. Шифрованием диска
г. Резервным копированием

10. Прочтите текст задания и выберите один верный ответ
Для обеспечения доступности АС при атаках типа DDoS используется:
Варианты ответов:
а. Антивирус
б. Система контроля целостности
в. Межсетевой экран нового поколения (NGFW) с функцией защиты от DDoS
г. Средство резервного копирования

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тестовые задания

Прочтите текст и установите последовательность
Упорядочите процесс развертывания защиты в АС:
Варианты ответов:
а. Анализ угроз безопасности
б. Выбор средств защиты
в. Интеграция в инфраструктуру
г. Обучение персонала
д. Непрерывный мониторинг

Прочтите текст и установите последовательность
Упорядочите этапы обеспечения целостности информации:
Варианты ответов:
а. Реагирование на нарушения
б. Определение критически важных данных
в. Настройка алгоритмов проверки
г. Мониторинг целостности
д. Установка средств контроля целостности

Прочтите текст и установите последовательность
Упорядочите процесс управления доступом:
Варианты ответов:
а. Авторизация3
б. Идентификация пользователей1
в. Аудит действий5
г. Аутентификация2
д. Контроль доступа4

Прочтите текст и установите последовательность
Упорядочите этапы защиты информационной системы от несанкционированного доступа:
Варианты ответов:
а. Установка систем обнаружения вторжений
б. Конфигурация межсетевых экранов
в. Применение криптографической защиты
г. Контроль и мониторинг
д. Анализ и реагирование на инциденты

Прочтите текст и установите последовательность
Упорядочите процесс обеспечения конфиденциальности:
Варианты ответов:
а. Классификация информации
б. Выбор средств шифрования
в. Внедрение средств защиты
г. Управление ключами
д. Контроль доступа к шифруемым данным

В2. Тематика рефератов и презентаций
1. Основные подходы к защите данных от НСД
2. Организация доступа к файлам
3. Фиксация доступа к файлам
4. Доступ к данным со стороны процесса
5. Особенности защиты данных от изменения

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Тестовые задания

Прочтите текст и вставьте пропущенное слово.
Для фильтрации сетевого трафика и предотвращения несанкционированного взаимодействия между сегментами автоматизированной системы используется _____.

Прочтите текст и вставьте пропущенное слово.
С целью подтверждения личности пользователя при входе в автоматизированную систему применяется процедура _____, которая может быть однофакторной или многофакторной.

Прочтите текст и вставьте пропущенное слово.

Для защиты рабочих станций АС от запуска вредоносного программного обеспечения применяется антивирусное ПО, использующее _____ базы для поиска известного вредоносного кода.

С2. Лабораторные работы

Лабораторная работа «Средства обеспечения безопасности ОС Windows»

Цель: изучить модель безопасности операционной системы Windows, получить навыки практического использования ее средств обеспечения безопасности.

ЛАБОРАТОРНАЯ РАБОТА №1. ЗАЩИТА ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ С ПОМОЩЬЮ МЕЖСЕТЕВОГО ЭКРАНА

Цель работы: Научиться конфигурированию межсетевого экрана D-link DFL-800T для приобретения навыков защиты локальной вычислительной сети предприятия от угроз информационной безопасности со стороны пользователей глобальной сети Интернет

ЛАБОРАТОРНАЯ РАБОТА №2. ОРГАНИЗАЦИЯ ЗАЩИЩЕННОЙ БЕСПРОВОДНОЙ КОМПЬЮТЕРНОЙ СЕТИ

Цель работы: Изучить порядок настройки беспроводной точки доступа и организации беспроводных сетей по технологии Wi-Fi.

Для проверки сформированности компетенции
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации

А1. Тестовые задания

1. Прочтите текст задания и выберите один верный ответ
Что является основной целью тестирования средств защиты информации?
Варианты ответов:
а. Проверка удобства интерфейса
б. Подтверждение соответствия заявленным функциям безопасности и выявление уязвимостей
в. Оценка скорости работы
г. Проверка совместимости с другими программами

2. Прочтите текст задания и выберите один верный ответ
Какой тип тестирования используется для проверки устойчивости средства защиты к реальным атакам?
Варианты ответов:
а. Функциональное тестирование
б. Тестирование на проникновение (Penetration Testing)
в. Регрессионное тестирование
г. Тестирование производительности

3. Прочтите текст задания и выберите один верный ответ
При тестировании брандмауэра, что нужно проверить в первую очередь?
Варианты ответов:
а. Скорость обработки пакетов
б. Правильность работы правил фильтрации трафика
в. Поддержку графического интерфейса
г. Объем занимаемой памяти

4. Прочтите текст задания и выберите один верный ответ
Что проверяют с помощью тестового файла EICAR?
Варианты ответов:
а. Работу резервного копирования
б. Работу шифрования
в. Функционирование антивирусного движка (способность обнаруживать тестовый вирус)
г. Работу брандмауэра

5. Прочтите текст задания и выберите один верный ответ
При тестировании системы обнаружения вторжений (IDS) используют:

Варианты ответов:

а. Резервные копии данных
б. Генераторы тестового трафика (например, инструменты вроде Metasploit, Nmap)
в. Средства шифрования
г. Антивирусные сканеры

6. Прочтите текст задания и выберите один верный ответ

Что проверяется при тестировании средства шифрования?

Варианты ответов:

а. Скорость шифрования
б. Криптографическая стойкость алгоритма и корректность работы ключей
в. Поддержка всех типов файлов
г. Размер интерфейса

7. Прочтите текст задания и выберите один верный ответ

Тестирование функции резервного копирования включает:

Варианты ответов:

а. Проверку скорости создания копии
б. Проверку успешности восстановления данных из резервной копии
в. Проверку сжатия архива
г. Проверку размера резервной копии

8. Прочтите текст задания и выберите один верный ответ

Что из перечисленного НЕ является методом тестирования средств защиты?

Варианты ответов:

а. Аудит безопасности
б. Тестирование на проникновение
в. Простое чтение инструкции
г. Моделирование атак

9. Прочтите текст задания и выберите один верный ответ

При тестировании системы контроля целостности (FIM) проверяют:

Варианты ответов:

а. Скорость сканирования
б. Способность обнаруживать изменения в защищаемых файлах и реестре
в. Возможность создания отчетов
г. Поддержку мультиязычности

10. Прочтите текст задания и выберите один верный ответ

Для тестирования средства аутентификации используется:

Варианты ответов:

а. Проверка скорости входа в систему

б. Проверка устойчивости к подбору пароля (брутфорс-тестирование) и защита передаваемых данных
в. Проверка цвета интерфейса
г. Проверка размера программы на диске

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тестовые задания

Прочтите текст и установите последовательность
Упорядочите этапы функционального тестирования средств защиты:
Варианты ответов:
а. Определение сценариев тестирования
б. Подготовка тестового окружения
в. Выполнение тестов
г. Документирование результатов
д. Устранение выявленных дефектов

Прочтите текст и установите последовательность
Упорядочите процесс тестирования криптографических функций:
Варианты ответов:
а. Проверка корректности алгоритма5
б. Шифрование данных2
в. Расшифровка данных3
г. Генерация тестовых данных1
д. Сравнение с исходными данными4

Прочтите текст и установите последовательность
Упорядочите этапы тестирования системы обнаружения вторжений:
Варианты ответов:
а. Подготовка сценариев атак
б. Анализ эффективности
в. Имитация атак
г. Создание тестовой инфраструктуры
д. Проверка обнаружения

Прочтите текст и установите последовательность
Упорядочите процесс тестирования механизмов аутентификации:
Варианты ответов:
а. Проверка результатов аутентификации4
б. Определение методов аутентификации1
в. Документирование уязвимостей5
г. Проведение попыток входа3
д. Подготовка тестовых учетных записей2

Прочтите текст и установите последовательность
Упорядочите этапы проверки производительности средств защиты:
Варианты ответов:

а. Установление метрик производительности
б. Создание нагрузочных сценариев
в. Выполнение тестирования
г. Анализ результатов
д. Оптимизация параметров

В2. Тематика рефератов и презентаций

6. Понятие ,безопасности компьютерных систем
7. Политика безопасности в корпоративных сетях. Оценка защищенности
8. Понятие ААА пользователя

Блок С. Задания практико-ориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Тестовые задания

Прочтите текст и вставьте пропущенное слово.
Для проверки корректности работы функций СЗИ на этапе приемки проводится тестирование на соответствие требованиям утвержденной _____ безопасности организации.

Прочтите текст и вставьте пропущенное слово.
Метод проверки СЗИ, заключающийся в преднамеренном создании условий, имитирующих действия злоумышленника, называется тестированием на _____.

Прочтите текст и вставьте пропущенное слово.
При тестировании функций целостности СЗИ проверяется способность средства защиты обнаруживать изменения в своих критических файлах путем сравнения их _____ сумм

С2. Лабораторные работы

ЛАБОРАТОРНАЯ РАБОТА №1. ОРГАНИЗАЦИЯ ЗАЩИЩЕННОЙ БЕСПРОВОДНОЙ КОМПЬЮТЕРНОЙ СЕТИ
Цель работы: Изучить порядок настройки беспроводной точки доступа и организации беспроводных сетей по технологии Wi-Fi.

ЛАБОРАТОРНАЯ РАБОТА №2. ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ПЕРЕХВАТА ТРАФИКА В КОМПЬЮТЕРНОЙ СЕТИ

Цель работы: Смоделировать попытку несанкционированного доступа к информации, которой обмениваются пользователи сети через FTP-сервер. Получить навыки перехвата и анализа пакетов компьютерной сети с помощью программы-монитора.

Для проверки сформированности компетенции
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств

А1. Тестовые задания

1. Прочтите текст задания и выберите один верный ответ

Наиболее надежный метод уничтожения конфиденциальной информации на жестком диске — это:

Варианты ответов:

а. Удаление файлов через «Корзину»
б. Форматирование диска
в. Физическое уничтожение (дезинтеграция, шредирование)
г. Перезапись нулями один раз

2. Прочтите текст задания и выберите один верный ответ

Какая утилита используется для безопасного удаления файлов в ОС Windows?

Варианты ответов:

а. `del`
б. `format`
в. SDelete (Sysinternals) или Eraser
г. CCleaner (без функции безопасного удаления)

3. Прочтите текст задания и выберите один верный ответ

Что означает термин «криптографическое стирание»?

Варианты ответов:

а. Удаление файлов без возможности восстановления
б. Перезапись данных зашифрованной информацией с последующим удалением ключа шифрования
в. Форматирование диска
г. Физическое повреждение носителя

4. Прочтите текст задания и выберите один верный ответ

При уничтожении информации на SSD-накопителе, почему простая перезапись неэффективна?

Варианты ответов:

а. SSD не поддерживают перезапись

б. SSD используют технологию выравнивания износа (wear leveling), и перезапись не затрагивает все ячейки
в. SSD слишком быстрые
г. На SSD нельзя установить утилиты

5. Прочтите текст задания и выберите один верный ответ
Какой стандарт определяет требования к безопасному уничтожению информации на носителях?
Варианты ответов:
а. ISO 27001
б. ГОСТ РВ 154-2012 / NIST SP 800-88
в. ГОСТ Р 54593-2011
г. RFC 2196

6. Прочтите текст задания и выберите один верный ответ
Для уничтожения информации на оптических дисках (CD/DVD) рекомендуется:
Варианты ответов:
а. Перезапись нулями
б. Удалить файлы
в. Физическое повреждение отражающего слоя (например, лазером или скрепкой)
г. Использование утилиты Eraser

7. Прочтите текст задания и выберите один верный ответ
Что обязательно делают с носителями, содержащими государственную тайну, после их эксплуатации?
Варианты ответов:
а. Передают на хранение
б. Уничтожают с составлением акта уничтожения под контролем уполномоченного лица
в. Форматируют и используют повторно
г. Продают

8. Прочтите текст задания и выберите один верный ответ
Что проверяют при верификации уничтожения информации?
Варианты ответов:
а. Скорость перезаписи
б. Отсутствие возможности восстановления данных специальными средствами (например, с помощью программ восстановления)
в. Размер носителя
г. Наличие вирусов

9. Прочтите текст задания и выберите один верный ответ

Сколько раз рекомендуется перезаписывать носитель случайными данными для надежного уничтожения информации (согласно стандартам)?
Варианты ответов:

а. 1 раз
б. 3–7 раз (в зависимости от стандарта, например, DoD 5220.22-M требует 3 проходов)
в. 10 раз
г. 100 раз

10. Прочтите текст задания и выберите один верный ответ

Что НЕЛЬЗЯ использовать для уничтожения информации на флеш-накопителях?
Варианты ответов:

а. Специализированные утилиты (например, Blaze)
б. Команда безопасного стирания (Secure Erase)
в. Простое удаление файлов или форматирование
г. Физическое разрушение

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тестовые задания

Прочтите текст и установите последовательность

Упорядочите процесс безопасного уничтожения данных на диске:
Варианты ответов:

а. Определение данных для уничтожения
б. Выбор метода перезаписи
в. Создание резервной копии (если требуется)
г. Выполнение процедуры уничтожения
д. Верификация уничтожения

Прочтите текст и установите последовательность

Упорядочите этапы уничтожения конфиденциальной информации:
Варианты ответов:

а. Физическое или программное уничтожение
б. Выбор средства уничтожения
в. Документирование процесса
г. Классификация информации
д. Инвентаризация носителей

Прочтите текст и установите последовательность

Упорядочите процесс утилизации носителей информации:
Варианты ответов:

а. Проверка наличия данных2
б. Выполнение уничтожения4
в. Определение типа носителя1

г. Составление акта об уничтожении5
д. Выбор метода уничтожения3

Прочтите текст и установите последовательность
Упорядочите этапы стирания данных из памяти устройства:
Варианты ответов:
а. Запуск процедуры стирания
б. Выбор устройства
в. Определение объема памяти для очистки
г. Проверка результатов
д. Выбор алгоритма перезаписи

Прочтите текст и установите последовательность
Упорядочите процесс уничтожения криптографических ключей:
Варианты ответов:
а. Подтверждение полного удаления
б. Локализация всех копий ключей
в. Выбор метода уничтожения
г. Подготовка оборудования
д. Выполнение процедуры уничтожения

В2. Тематика рефератов и презентаций
1. Понятие уязвимости компьютерных систем
2. Политика безопасности в компьютерных системах. Оценка
3. защищенности
4. Понятие идентификации пользователя

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Тестовые задания
Прочтите текст и вставьте пропущенное слово.
Программное удаление данных, исключающее их восстановление программными методами, осуществляется путем многократной _____ секторов носителя случайными последовательностями бит.

Прочтите текст и вставьте пропущенное слово.
Для гарантированного уничтожения данных на магнитных жестких дисках (HDD) без разрушения корпуса применяются устройства, генерирующие мощное электромагнитное поле, — _____.

Прочтите текст и вставьте пропущенное слово.

Полное физическое уничтожение твердотельных накопителей (SSD) или оптических дисков путем превращения их в мелкую фракцию производится с помощью специального устройства — _____.

Прочтите текст и вставьте пропущенное слово.

Стандартная очистка данных на SSD-накопителях требует подачи специальной команды _____, так как обычная перезапись из-за алгоритмов выравнивания износа не гарантирует удаление данных из всех ячеек

С2. Лабораторные работы

Лабораторная работа «Средства обеспечения безопасности ОС Windows»

Цель: изучить модель безопасности операционной системы Windows, получить навыки практического использования ее средств обеспечения безопасности.

ЛАБОРАТОРНАЯ РАБОТА №1. ЗАЩИТА ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ С ПОМОЩЬЮ МЕЖСЕТЕВОГО ЭКРАНА

Цель работы: Научиться конфигурированию межсетевого экрана D-link DFL-800T для приобретения навыков защиты локальной вычислительной сети предприятия от угроз информационной безопасности со стороны пользователей глобальной сети Интернет

ЛАБОРАТОРНАЯ РАБОТА №2. ЗАЩИТА ПЕРЕДАВАЕМЫХ ДАННЫХ ПОМОЩЬЮ ШИФРОВАНИЯ И ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Цель работы: Приобрести навыки защиты и верификации передаваемых данных с помощью механизма шифрования и электронной цифровой подписи, используя программный продукт КриптоАРМ.

Основные сведения о программе КриптоАРМ

ЛАБОРАТОРНАЯ РАБОТА №3. РАБОТА С ЗАЩИЩЕННЫМИ ДИСКАМИ

Цель работы: Приобрести навыки работы с защищенными дисками на локальной рабочей станции с помощью программного пакета Secret Disk.

Для проверки сформированности компетенции
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

Блок А. Задания репродуктивного уровня («знать»)

А1. Тестовые задания

1. Прочтите текст задания и выберите один верный ответ
Система, которая централизованно собирает, анализирует и коррелирует события безопасности из разных источников, называется:
Варианты ответов:
а. Антивирус
б. IDS
в. SIEM (Security Information and Event Management)
г. Firewall

2. Прочтите текст задания и выберите один верный ответ
Какие события обязательно регистрируются в журнале безопасности?
Варианты ответов:
а. Запуск приложений
б. Попытки входа в систему, доступ к критичным ресурсам, изменения в политиках безопасности
в. Открытие веб-страниц
г. Установка программ

3. Прочтите текст задания и выберите один верный ответ
Что делает система обнаружения вторжений (IDS)?
Варианты ответов:
а. Блокирует атаки
б. Обнаруживает подозрительную активность путем анализа сетевого трафика и/или системных журналов и генерирует оповещения
в. Шифрует журналы
г. Выполняет резервное копирование

4. Прочтите текст задания и выберите один верный ответ
Что из перечисленного является алертом (alert) в системах безопасности?
Варианты ответов:
а. Информационное сообщение
б. Предупреждение о подозрительном или злонамеренном событии
в. Отчет о производительности

г. Ошибка в работе ПО

5. Прочтите текст задания и выберите один верный ответ
Функция корреляции событий в SIEM-системе позволяет:
Варианты ответов:
а. Удалять дубликаты событий
б. Объединять связанные события из разных источников для выявления комплексных атак (например, последовательность действий)
в. Шифровать журналы
г. Сжимать данные

6. Прочтите текст задания и выберите один верный ответ
Что нужно сделать при получении алерта от IDS о возможной атаке?
Варианты ответов:
а. Проигнорировать
б. Провести расследование инцидента: подтвердить факт атаки, выявить масштаб и принять меры ликвидации
в. Немедленно отключить сервер
г. Удалить алерт

7. Прочтите текст задания и выберите один верный ответ
Средство, которое автоматически реагирует на атаки (например, блокирует IP-адрес атакующего), называется:
Варианты ответов:
а. IDS
б. SIEM
в. IPS (Intrusion Prevention System) или SOAR (Security Orchestration, Automation and Response)
г. Антивирус

8. Прочтите текст задания и выберите один верный ответ
Для чего используется аудит событий безопасности?
Варианты ответов:
а. Для контроля рабочего времени сотрудников
б. Для расследования инцидентов безопасности и соответствия требованиям регуляторов (например, ФСТЭК, GDPR)
в. Для оптимизации производительности
г. Для резервного копирования

9. Прочтите текст задания и выберите один верный ответ
Что рекомендуется делать с журналами событий безопасности?
Варианты ответов:
а. Удалять через месяц

б. Регулярно архивировать и хранить в защищенном месте в течение установленного срока
в. Оставлять только последние 10 записей
г. Передавать коллегам

10. Прочтите текст задания и выберите один верный ответ
Какое программно-аппаратное средство позволяет фиксировать действия пользователя за компьютером в реальном времени для последующего расследования инцидентов?
Варианты ответов:
а. Антивирус
б. Система контроля целостности
в. Система регистрации действий пользователя (User Activity Monitoring — UAM) или keylogger (только по согласованию с законом!)
г. Межсетевой экран

А2.Вопросы для обсуждения
1. Каковы процедуры инициализации объекта информационной защиты?
2. Опишите типовые схемы идентификации и аутентификации пользователя.
3. Каковы недостатки и достоинства схемы простой аутентификации с помощью пароля?
4. Достоинства биометрических методов идентификации и аутентификации пользователя по сравнению с традиционными?
Основополагающие меры комплексной безопасности АС.
5. Основные подходы при проектировании.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тестовые задания

Прочтите текст и установите последовательность
Упорядочите процесс организации логирования событий:
Варианты ответов:
а. Определение событий для регистрации
б. Установка средств логирования
в. Конфигурация параметров логирования
г. Включение логирования
д. Мониторинг логов

Прочтите текст и установите последовательность
Упорядочите этапы анализа логов безопасности:
Варианты ответов:
а. Создание отчета о происшествиях
б. Сбор логов из различных источников

в. Нормализация формата данных
г. Корреляция событий
д. Выявление аномалий

Прочтите текст и установите последовательность
Упорядочите процесс реагирования на обнаруженную атаку:
Варианты ответов:
а. Изоляция затронутых систем
б. Обнаружение атаки
в. Восстановление и закрытие инцидента
г. Классификация угрозы
д. Анализ причин и способов входа

Прочтите текст и установите последовательность
Упорядочите этапы настройки системы обнаружения вторжений:
Варианты ответов:
а. Установка консоли управления3
б. Тестирование функциональности5
в. Конфигурация датчиков2
г. Определение сигнатур атак1
д. Настройка оповещений4

Прочтите текст и установите последовательность
Упорядочите процесс ликвидации последствий компьютерной атаки:
Варианты ответов:
а. Восстановление из резервных копий
б. Остановка атаки и изоляция систем
в. Проверка целостности данных
г. Анализ повреждений
д. Внедрение защитных мер от повторной атаки

В2. Тематика рефератов и презентаций
1. Построение программно-аппаратных комплексов шифрования
2. Проблема защиты отчуждаемых компонентов
3. Надежность средств защиты компонент
4. Несанкционированное копирование программ
5. Подходы к задаче защиты от копирования
6. Организация хранения ключей
7. Обратное проектирование ПО
8. Задачи защиты от изучения и способы их решения
9. Компьютерные вирусы

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Тестовые задания

Прочтите текст и вставьте пропущенное слово.

Автоматизированный сбор, корреляция и анализ событий безопасности из различных источников в режиме реального времени осуществляется системами класса _____.

Прочтите текст и вставьте пропущенное слово.

Программно-аппаратные средства, предназначенные для активного вмешательства в сетевой трафик с целью блокировки обнаруженной атаки, называются системами _____ вторжений.

Прочтите текст и вставьте пропущенное слово.

Процесс ведения хронологической записи операций в информационной системе, позволяющий восстановить последовательность действий пользователей, называется _____.

Прочтите текст и вставьте пропущенное слово.

При обнаружении подозрительной активности система обнаружения вторжений генерирует _____, оповещая администратора о возможной попытке несанкционированного доступа

С2. Лабораторные работы

Лабораторная работа № 1 .

Тема: «Основные функции средств защиты от копирования**»**

Цель работы: Познакомится с основными функциями средств защиты от копирования.

Задание для работы:

1. Защита от копирования
2. Функции средств защиты

Лабораторная работа № 2.

Тема: «Виды мероприятий по защите информации**»**

Цель работы: Познакомится с различными видами мероприятий по защите информации.

Задание для работы:

1. Защита информации, обрабатываемой ПЭВМ и ЛВС, от утечки по сети электропитания
2. Защита программ и данных от несанкционированного копирования

Лабораторная работа № 3.

Тема: «Современные системы защиты пэвм от несанкционированного доступа к информации**»**
Цель работы: Познакомится с различными современными системами защиты пэвм от несанкционированного доступа к информации.
Задание для работы:
1. Системы защиты ПЭВМ.
2. Несанкционированный доступ к информации

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1.Перечень экзаменационных вопросов

1. Основные принципы создания средств защиты информации.
2. Описать способ контроля потоков данных, посредством применения основного правила разграничения доступа, применяемого в мандатном механизме управлениядоступом
3. Концепция построения программно–аппаратных средств обеспечения информационной безопасности.
4. Описать применение ролевого способа управления доступом.
5. Методы ограничения доступа и управления доступом. Идентификация и аутентификация. Парольные системы.
6. Указать основные документы, определяющие требования к структуре и функциям СЗИ.
7. Методы ограничения доступа и управления доступом. Дискреционное управление доступом.
8. Описать порядок функционирования компонентов СЗИ от НСД Secret Net.
9. Методы ограничения доступа и управления доступом. Мандатное управлениедоступом.
10. Описать порядок функционирования ядра и основных подсистем СЗИ от НСДSecret Net.
11. Методы ограничения доступа и управления доступом. Ролевое управлениедоступом
12. Дать характеристику режимов идентификации и аутентификации, реализуемых СЗИ от НСД Secret Net

13. Структура и функции программно–аппаратных средств обеспечения информационной безопасности.
14. Описать применение механизма блокировок компьютера и видов блокировок, реализуемых СЗИ от НСД Secret Net, дать их сравнительную характеристику.
15. Назначение, режимы функционирования, основные функции, состав устанавливаемых компонентов СЗИ от НСД Secret Net
16. Описать процедуру доверенной загрузки операционной системы при применении электронных замков и устройствовводаидентификационныхпризнаков (УВИП).
17. Подсистемы клиента СЗИ от НСД Secret Net: ядро системы защиты, подсистема локального управления, защитные подсистемы
18. Описать общий порядок функционирования СЗИ от НСД Страж NT
19. Подсистемы клиента СЗИ от НСД Secret Net: модуль входа, подсистема контроля целостности, подсистема работы с аппаратной поддержкой
20. Описать порядок настройки подсистемы дискреционного и мандатного управления доступом СЗИ от НСД Страж NT
21. Защитные механизмы СЗИ от НСД Secret Net. Идентификация и аутентификация пользователей.
22. Описать порядок тестирования, восстановления и обеспечения целостности СЗИ от НСД Страж NT.
23. Функционирование подсистемы учета носителей СЗИ от НСД Страж NT.
24. Определить возможную конфигурацию аппаратных средств СЗИ от НСД SecretNet, применяемых для идентификации и аутентификации пользователей.
25. Определения и классификацию устройств ввода идентификационных признаков (УВИП).
26. Пояснить применение концепций распространения прав доступа и дать их сравнительную характеристику.
27. Устройства ввода идентификационных признаков. Устройства iButton.

28. Пояснить результаты применения правил выбора стойких паролей.
29. Устройства ввода идентификационных признаков. Смарт-карты. Устройства ввода на базе смарт-карт.
30. Дать сравнительную характеристику основных подходов к разработке средств защиты информации.
31. Устройства ввода идентификационных признаков. USB-ключи.
32. Пояснить применение концепции диспетчера доступа.
33. Устройства ввода идентификационных признаков. Комбинированные УВИП. Электронные замки. Общий алгоритм функционирования
34. Дать характеристику основных принципов создания средств защиты информации и их применения
35. Назначение, режимы функционирования, основные функции, состав устанавливаемых компонентов СЗИ от НСД Secret Net
36. Описать процедуру доверенной загрузки операционной системы при применении электронных замков и устройствовводаидентификационныхпризнаков (УВИП).
37. Дать характеристику режимов идентификации и аутентификации, реализуемых СЗИ от НСД Secret Net.
38. Указать основные документы, определяющие требования к структуре и функциям СЗИ.

РАЗДЕЛ 3.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Балльно-рейтинговая система является базовой системой оценивания сформированности компетенций обучающихся.очной формы обучения.

Итоговая оценка сформированности компетенции(й) обучающихся в рамках балльно-рейтинговой системы осуществляется в ходе текущего контроля успеваемости, промежуточной аттестации и определяется как сумма баллов, полученных обучающимися в результате прохождения всех форм контроля.

Оценка сформированности компетенции(й) по междисциплинарному курсу складывается из двух составляющих:

✓ первая составляющая – оценка преподавателем сформированности компетенции(й) в течение семестра в ходе текущего контроля успеваемости (максимум 100 баллов). Структура первой составляющей определяется технологической картой дисциплины, которая в начале семестра доводится до сведения обучающихся;

✓ вторая составляющая – оценка сформированности компетенции(й) обучающихся на экзамене (максимум – 30 баллов).

Для студентов очно-заочной формы обучения применятся 4-балльная и бинарная шкалы оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся.

уровни освоения компетенций	продвинутый уровень	базовый уровень	пороговый уровень	допороговый уровень
100 – балльная шкала	85 и ≥	70 – 84	51 – 69	0 – 50
4 – балльная шкала	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»

Шкала оценок при текущем контроле успеваемости по различным показателям

Показатели оценивания сформированности компетенций	***Баллы***	***Оценка***
Выполнение лабораторных работ	0-20	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Ответы на устные вопросы	0-10	«неудовлетворительно» «удовлетворительно»

		«хорошо» «отлично»
Тестирование	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение и публичная защита реферата	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение презентаций	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по текущему контролю успеваемости

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-50	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины
51-69	«удовлетворительно»	Пороговый уровень	Не менее 50% заданий, подлежащих текущему контролю успеваемости, выполнены без существенных ошибок
70-84	«хорошо»	Базовый уровень	Обучающимся выполнено не менее 75% заданий, подлежащих текущему контролю успеваемости, или при выполнении всех заданий допущены незначительные ошибки; обучающийся показал владение навыками систематизации материала и применения его при решении практических заданий; задания выполнены без ошибок
85-100	«отлично»	Продвинутый уровень	100% заданий, подлежащих текущему контролю успеваемости, выполнены самостоятельно и в требуемом объеме; обучающийся проявляет умение обобщать, систематизировать материал

			и применять его при решении практических заданий; задания выполнены с подробными пояснениями и аргументированными выводами

Шкала оценок по промежуточной аттестации

Наименование формы промежуточной аттестации	***Баллы***	***Оценка***
Экзамен	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации обучающихся

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-9	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на вопросы
10-16	«удовлетворительно»	Пороговый уровень	Обучающийся дал неполные ответы на вопросы, с недостаточной аргументацией, практические задания выполнены не полностью, компетенции, осваиваемые в процессе изучения дисциплины сформированы не в полном объеме.
17-23	«хорошо»	Базовый уровень	Обучающийся в целом приобрел знания и умения в рамках осваиваемых в процессе обучения по междисциплинарному курсу компетенций; обучающийся ответил на все вопросы, точно дал определения и понятия, но затрудняется подтвердить теоретические положения практическими примерами; обучающийся показал хорошие знания

			по предмету, владение навыками систематизации материала и полностью выполнил практические задания
25-30	«отлично»	Продвинутый уровень	Обучающийся приобрел знания, умения и навыки в полном объеме, закрепленном рабочей программой дисциплины; терминологический аппарат использован правильно; ответы полные, обстоятельные, аргументированные, подтверждены конкретными примерами; обучающийся проявляет умение обобщать, систематизировать материал и выполняет практические задания с подробными пояснениями и аргументированными выводами

РАЗДЕЛ 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций

Тестирование проводится с помощью системы дистанционного обучения «Прометей», входящей в состав электронной информационно-образовательной среды Дагестанского государственного университета народного хозяйства.

На тестирование отводится 45 минут. Каждый вариант тестовых заданий включает 30 вопросов.

Методика оценивания выполнения тестов

Баллы	Оценка	Показатели	Критерии
25-30	«отлично»	1. Полнота выполнения тестовых заданий; 2. Своевременность выполнения; 3. Правильность ответов на вопросы; 4. Самостоятельность тестирования; 5. и т.д.	Выполнено более 85 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос
19-24	«хорошо»		Выполнено более 70 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос; однако были допущены неточности в определении понятий, терминов и др.

15-18	«удовлетворительно»		Выполнено более 54 % заданий предложенного теста, в заданиях открытого типа дан неполный ответ на поставленный вопрос, в ответе не присутствуют доказательные примеры, текст со стилистическими и орфографическими ошибками.
0-14	«неудовлетвори-тельно»		Выполнено не более 53 % заданий предложенного теста, на поставленные вопросы ответ отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях).

Устный опрос проводится в первые 15 минут занятий семинарского типа в формате обсуждения с названными преподавателем студентами. Остальные обучающиеся вправе дополнить или уточнить ответ по своему желанию (соблюдаю очередность ответа). Основной темой для опроса являются вопросы для обсуждения, соответствующие теме предыдущей лекции, но преподаватель может уточнять задаваемый вопрос, задавать наводящие вопросы или сужать вопрос до отдельного аспекта обсуждаемой темы.

Методика оценивания ответов на устные вопросы

Баллы	***Оценка***	**Показатели**	**Критерии**
9-10	«отлично»	1. Полнота данных ответов; 2. Аргументированность данных ответов; 3. Правильность ответов на вопросы; 4. и т.д.	Полно и аргументировано даны ответы по содержанию задания. Обнаружено понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные. Изложение материала последовательно и правильно.
7-8	«хорошо»		Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.
5-6	«удовлетворительно»		Студент обнаруживает знание и понимание основных

			положений данного задания, но: 1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки.
0-4	«неудовлетвори-тельно»		Студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал; отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом.

Тема реферата выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На написание реферата отводится одна неделя. Реферат оформляется согласно действующим в Дагестанском государственном университете народного хозяйства требованиям к оформлению письменных работ. Объем представленного реферата должен быть не менее 10 страниц машинописного текста без учета титульного листа.

Публичная защита реферата проводится в присутствии остальных студентов, защищающих рефераты. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель реферата, а также цельно сформулировать базовую идею, отраженную в реферате.

Методика оценивания выполнения рефератов

Баллы	Оценка	Показатели	Критерии
5	«отлично»	1. Полнота выполнения рефератов; 2. Своевременность выполнения; 3. Правильность	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ

		ответов на вопросы.	различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.
3-4	«хорошо»		Основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.
1-2	«удовлетворительно»		Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы.
0	«неудовлетвори-тельно»		Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы

Тема презентации выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На подготовку презентации отводится одна неделя.

Публичная презентация проводится в присутствии остальных студентов. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель презентации, а также цельно сформулировать базовую идею.

Методика оценивания выполнения презентаций

Баллы	**Оценка**	***Показатели***	***Критерии***
5	«отлично»	1. Полнота выполнения	Выполнены все требования к

		презентаций; 2. Своевременность выполнения; 3. Правильность ответов на вопросы; 4. и т.д.	составлению презентаций: дизайн слайдов, логика изложения материала, текст хорошо написан и сформированные идеи ясно изложены и структурированы
3-4	«хорошо»		Основные требования к презентациям выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем презентации
1-2	«удовлетворительно»		Имеются существенные отступления от требований к презентациям. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании презентаций или при ответе на дополнительные вопросы.
0	«неудовлетвори-тельно»		Тема презентации не раскрыта, обнаруживается существенное непонимание проблемы

Лабораторные работы выполняются в специализированной аудитории во время лабораторных занятий. Предусмотрено выполнение одной лабораторной работы в течение одного занятия согласно текущей тематике. Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности полученного результата. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения шагов лабораторной работы, то это негативно отражается на оценке выполняющего задание студента.

Методика оценивания лабораторных работ

Баллы	***Оценка***	**Показатели**	**Критерии**
18-20	«отлично»	1. Полнота выполнения заданий 2. Выполнение дополнительных заданий	- правильно выполнены все задания лабораторной работы в соответствии с требованиями; - правильно выполнены дополнительные задания; - своевременно предоставлен

		3. Подготовка отчета	отчет о выполнении работы.
14-17	«хорошо»		- правильно выполнены все задания в основной части; - дополнительные задания выполнены не в полном объеме; - предоставлен отчет о выполнении работы, либо в случае несвоевременного предоставления отчета или с наличием несущественных ошибок в выполнении лабораторных заданиях
11-13	«удовлетворительно»		- выполнены не все, но более 50% заданий лабораторной работы; - дополнительные задания не выполнены, - несвоевременно предоставлен отчет о выполнении работы.
0-10	«неудовлетвори-тельно»		- выполнено менее 50% лабораторной работы; - не выполнены дополнительные задания; - отчет о выполнении работы не предоставлен

Процедура промежуточной аттестации проходит в соответствии с Положением о промежуточной аттестации знаний студентов и учащихся ДГУНХ.

Аттестационные испытания проводятся преподавателем, ведущим лекционные занятия по данной междисциплинарному курсу, или преподавателями, ведущими практические и лабораторные занятия (кроме устного экзамена). Присутствие посторонних лиц в ходе проведения аттестационных испытаний без разрешения ректора или проректора по учебной работе не допускается (за исключением работников университета, выполняющих контролирующие функции в соответствии со своими должностными обязанностями). В случае отсутствия ведущего преподавателя аттестационные испытания проводятся преподавателем, назначенным письменным распоряжением по кафедре (структурному подразделению).

Инвалиды и лица с ограниченными возможностями здоровья, имеющие нарушения опорно-двигательного аппарата, допускаются на аттестационные испытания в сопровождении ассистентов-сопровождающих.

Во время аттестационных испытаний обучающиеся могут пользоваться программой дисциплины, а также с разрешения преподавателя справочной и нормативной литературой, непрограммируемыми калькуляторами.

Лист актуализации оценочных материалов по междисциплинарному курсу «Программно-аппаратные средства защиты информации»

Фонд оценочных средств пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Фонд оценочных средств пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Фонд оценочных средств пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Фонд оценочных средств пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____