ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»

Утверждены решением
Ученого совета ДГУНХ,
протокол № 9
от 24 марта 2025 г

КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ПО ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»

НАПРАВЛЕНИЕ ПОДГОТОВКИ
10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПРОФИЛЬ «БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Уровень высшего образования - бакалавриат

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00C5A9FA0FAD6D6153888A98846B419FD3
Владелец: Бучаев Ахмед Гамидович
Действителен: с 11.07.2024 до 04.10.2025

Махачкала – 2025

УДК 681.518(075.8)
ББК 32.81.73

Составитель – Гасанова Зарема Ахмедовна, кандидат педагогических наук, и.о. зав. кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

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

Внешний рецензент – Абдуллаев Ших-Саид Омаржанович, доктор технических наук, главный научный сотрудник Отдела математики и информатики Дагестанского научного центра Российской академии наук.

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

Оценочные материалы по дисциплине «Безопасность операционных систем» разработаны в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г., № 1427, в соответствии с приказом Министерства науки и высшего образования Российской Федерации от 6.04.2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»

Оценочные материалы по дисциплине «Безопасность операционных систем» размещены на официальном сайте www.dgunh.ru

Гасанова З.А. Оценочные материалы по дисциплине «Безопасность операционных систем» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2025 г. – 34 с.

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

Рекомендованы к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрены на заседании кафедры «Информационные технологии и информационная безопасность» 24 февраля 2025 г., протокол № 70.

.

СОДЕРЖАНИЕ

Назначение оценочных материалов……..4

РАЗДЕЛ 1. Перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины ….…….…….5

1.1 Перечень формируемых компетенций……5

1.2 Перечень компетенций с указанием видов оценочных средств…….5

РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по дисциплине……8

РАЗДЕЛ 3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания……..26

РАЗДЕЛ 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций…….29

Лист актуализации оценочных материалов по дисциплине……. 34

Назначение оценочных материалов

Оценочные материалы для текущего контроля успеваемости (оценивания хода освоения дисциплин), для проведения промежуточной аттестации (оценивания промежуточных и окончательных результатов обучения по дисциплине) обучающихся по дисциплине «Безопасность операционных систем» на соответствие их учебных достижений поэтапным требованиям образовательной программы высшего образования 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем»

Оценочные материалы по дисциплине «Безопасность операционных систем» 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.

Оценочные материалы 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	**Профессиональные компетенции**
ПК-1.	Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей

1.2. Перечень компетенций с указанием видов оценочных средств

Формируемые компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций***	***Уровни освоения компетенций***	***Критерии оценивания сформированности компетенций***	***Виды оценочных средств***
ПК-1. Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами	ИПК-1.1. Администрирует подсистему защиты информации операционных систем	**Знать:** – основные приемы настройки подсистем информационной безопасности операционных систем - принципы построения подсистем защиты в операционных системах	Пороговый уровень	Обучающийся слабо (частично) знает основные приемы настройки подсистем информационной безопасности операционных систем, принципы построения подсистем защиты в операционных системах	**Блок А –** задания репродуктивного уровня – тестовые задания; – вопросы для устного опроса
			Базовый уровень	Обучающийся с не-значительными ошибками и отдельными пробелами знает основные приемы настройки подсистем информационной безопасности операционных систем, принципы построения подсистем защиты в операционных системах	
			Продвинутый	Обучающийся с требуемой степенью	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
данных и компьютерных сетей			уровень	полноты и точности знает основные приемы настройки подсистем информационной безопасности операционных систем, принципы построения подсистем защиты в операционных системах	
		<u>Уметь:</u> - пользоваться средствами защиты, предоставляемыми операционной системой - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты – планировать политику безопасности операционной системы.	Пороговый уровень	Обучающийся слабо (частично) умеет пользоваться средствами защиты, предоставляемыми операционной системой, осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты, планировать политику безопасности операционной системы	**Блок В** – задания реконструктивного уровня – тематика рефератов; - тематика презентаций.
			Базовый уровень	Обучающийся с незначительными затруднениями умеет пользоваться средствами защиты, предоставляемыми операционной системой, осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты, планировать	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				политику безопасности	
			Продвинутый уровень	Обучающийся умеет пользоваться средствами защиты, предоставляемыми операционной системой, осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты, планировать политику безопасности	
		Владеть: – методами и инструментарием конфигурирования и настройки средств защиты информации в ОС	Пороговый уровень	Обучающийся слабо (частично) владеет методами и инструментарием конфигурирования и настройки средств защиты информации в ОС	**Блок С** – задания практико-ориентированного уровня – лабораторные работы.
			Базовый уровень	Обучающийся с небольшими затруднениями владеет методами и инструментарием конфигурирования и настройки средств защиты информации в ОС	
			Продвинутый уровень	Обучающийся свободно владеет методами и инструментарием конфигурирования и настройки средств защиты информации в ОС	

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

Для проверки сформированности компетенции ПК-1. Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей
ИПК-1.1. Администрирует подсистему защиты информации операционных систем

Блок А. Задания репродуктивного уровня («знать»)

А.1 Тестовые задания по дисциплине

1. Несанкционированный доступ – это …
   А. доступ или воздействие с нарушением правил доступа;
   Б. изменение пароля с правами администратора;
   В. доступ в незащищенную систему пользователя;
   Г. изменение пароля доступа в систему пользователем.
2. Потенциальная возможность определенным образом нарушить информационную безопасность это:
   А. атака
   Б. уязвимость
   В. угроза
   Г. Риск
3. Попытка реализации угрозы – это …
   А. уязвимость;
   Б. атака;
   В. конфиденциальность;
   Г. взлом.

4. Угроза утечки информации ограниченного доступа, хранящейся в информационной системе или передающейся по каналам связи – это …
   А. угроза нарушения конфиденциальности
   Б. угроза нарушения целостности
   В. угроза отказа служб
   Г. все перечисленные
5. Какие методы несанкционированного доступа является наиболее распространёнными в операционной системе Windows?
   А. Позволяющие несанкционированно запустить исполняемый код
   Б. Позволяющие обойти установленные разграничения прав доступа
   В. Троянские программы
   Г. Позволяющие осуществить несанкционированные операции чтения/записи файловых и других объектов

6. К типовым функциональным дефектам ОС не относится:
   А. Идентификация
   Б. Аутентификация
   В. Список паролей
   Г. Подразумеваемое доверие
7. Наиболее распространенная группа атак на ОС Windows:
   А. «Троянские программы»
   Б. DoS-атаки
   В. Атаки на пароль
   Г. Закладки

8. Какие сведения не содержит системный реестр Windows:
   А. Профили пользователей
   Б. Данные об установленных программах и типов документов, создаваемых каждой программой
   В. Данные об используемой памяти
   Г. Данные об используемых портах

9. Установите соответствия:

1. HKEY_CLASSES_ROOT	А. Здесь содержатся настройки оболочки пользователя (например, Рабочего стола, меню "Пуск", ...), вошедшего в Windows
2. HKEY_CURRENT_USER	Б. Содержит конфигурационные данные для текущего аппаратного профиля. Аппаратные профили представляют собой наборы изменений, внесенных в стандартную конфигурацию сервисов и устройств, установленную данными разделов Software и System корневого раздела HKEY_LOCAL_MACHINE.
3. HKEY_LOCAL_MACHINE	В. Эта ветвь содержит индивидуальные настройки каждого пользователя компьютера, каждый пользователь представлен под ключом SID, расположенном под главной ветвью.
4. HKEY_USERS	Г. В этом разделе содержится информация о зарегистрированных в Windows типах файлов, что позволяет открывать их по двойному щелчку мыши, а также информация для OLE и операций drag-and-drop

5. HKEY_CURRENT_CONFIG	Д. Этот раздел содержит информацию, относящуюся к компьютеру: драйверы, установленное программное обеспечение и его настройки. Содержит настройки оболочки Windows для всех пользователей.

10. Реестр состоит из…
    A. ключей и их значений
    B. ключей и параметров
    C. ключей, подключей и параметров

11. Отличие ульев от других групп ключей состоит в том, что
    A. они изменяются при загрузке ОС
    B. они являются постоянными компонентами реестра
    C. часть ульев постоянна, а часть меняется в ходе работы ОС

12. Утилита, позволяющая редактировать права доступа пользователей к отдельным ключам реестра
A. reg.exe
    B. regedit.exe
    C. regini.exe

13. Для чего требуется резервное копирование реестра?
A. Для восстановления файловой системы
B. Для защиты от вирусов
C. Для предотвращения краха системы

14. Каких групп параметров реестра не существует:
D. строковые
E. числовые
F. двоичные
G. DWORD

15. Какие из перечисленных программных продуктов предназначены для работы с реестром Windows:
    A. CCleaner
    B. Reg Organizer
    C. Red Studio
    D. Clearsoft

16. Идентификация - это:
A. процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе.
B. предоставление личных данных пользователем

C. процедура, в результате которой субъект получает определенные права в системе
D. метод хранения логина и пароля

17. Аутентификация - это:
A. проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользователей;
B. подтверждение подлинности электронного письма путём проверки цифровой подписи письма по открытому ключу отправителя;
C. проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла.
D. проверка пользователем введенных им данных

18. Укажите способы усиления парольной защиты, связанные с использованием только политик безопасности ОС (несколько вариантов):
A. увеличение длины пароля
B. использование устройств авторизации
C. установка параметров сложности пароля
D. использование биометрической авторизации

19. Отсутствие настройки по какому параметру может привести к бесполезности параметра «Требовать неповторяемости паролей»?
A. Максимальный срок действия пароля
B. Минимальная длина пароля
C. Минимальный срок действия пароля
D. Пароль должен отвечать требованиям сложности

20. Чем обусловлено требование неповторяемости паролей?
A. Пароль не должен повторять логин пользователя
B. У всех пользователей должны быть разные пароли
C. Пароль должен отличаться от нескольких предыдущих
D. В пароле не должно быть одинаковых сегментов

21. Процесс авторизации - это процесс
A. ввода пользователем логина и пароля
B. доказательство того, что пользователь тот, за кого выдает
C. предоставления пользователю прав на выполнение определѐнных действий
D. получения идентификатора пользователя в системе

22. Разграничение доступа к ресурсам:
A. порядок использования ресурсов автоматизированной системы, при котором осуществляется ограничение доступа субъектов к объектам системы

B. порядок использования ресурсов автоматизированной системы, при котором субъекты получают доступ к объектам системы в строгом соответствии с установленными правилами
C. порядок использования ресурсов автоматизированной системы, при котором объекты получают доступ к субъектам системы в строгом соответствии с установленными правилами.
D. порядок использования ресурсов автоматизированной системы, при котором осуществляется ограничение доступа к ресурсам системы

23. Активным компонентом системы является:
A. Объект
B. Субъект
C. Процесс
D. Ресурс

24. В мандатной модели доступа метки доступа определяют:
A. Уровень секретности
B. Уровень доступа
C. Гриф секретности

25. В мандатной модели доступа субъект может читать информацию только из объекта уровень секретности которого:
A. не выше уровня секретности субъекта
B. выше уровня секретности субъекта
C. не ниже уровня секретности субъекта
D. ниже уровня секретности субъекта

26. В мандатной модели доступа субъект может записывать информацию в объекты только:
A. своего уровня
B. своего уровня или более низких уровней секретности
C. своего уровня или более высоких уровней секретности
D. более низких уровней секретности

27. В модели дискреционного разграничения доступа права доступа к объекту устанавливает:
A. Администратор
B. Владелец
C. Субъект
D. Операционная система

28. Модель, характеризующаяся разграничением доступа между поименованными субъектами и объектами:
A. Модель ролевого разграничения

B. Модель систем дискреционного разграничения доступа
C. Мандатная модель разграничения доступа

29. Дескриптор безопасности, содержащий информацию о владельце объекта:
A. GID
B. UID
C. SID
D. OID

30. Механизм контроля доступа обеспечивает:
A. контроль учетных записей пользователей, прохождение ими процедур идентификации и аутентификации
B. разрешение или запрет работы с файлами, каталогами, устройствами, таблицами, полями и записями базы данных, сетевыми ресурсами
C. проверку неизменности контролируемых объектов в соответствии с заданным эталоном
D. фиксацию действий пользователей, доступа процессов к защищаемым ресурсам
E. применение средств криптографической защиты информации

31. Укажите виды разрешений на работу с объектами в рамках дискреционной
модели доступа. (несколько вариантов)
A. чтение и запись
B. выполнение
C. просмотр
D. чтение конфиденциальных документов и запись информации в них

32. Механизм аудита обеспечивает:
A. контроль учетных записей пользователей, прохождение ими процедур идентификации и аутентификации
B. разрешение или запрет работы с файлами, каталогами, устройствами, таблицами, полями и записями базы данных, сетевыми ресурсами
C. проверку неизменности контролируемых объектов в соответствии с заданным эталоном
D. фиксацию действий пользователей, доступа процессов к защищаемым ресурсам

33. Аудит ОС заключается в :
A. фиксации всех событий, от которых зависит безопасность системы
B. безопасном входе в систему
C. контроле доступа к файлам и папкам
D. средствах защиты от замены файлов

34. Какую оснастку необходимо добавить в консоль управления, чтобы провести анализ безопасности операционной системы?
    A. Монитор IP-безопасности
    B. Системный монитор
    C. Анализ и настройка безопасности
    D. Редактор объектов групповой политики

35. Какой тип объектов не фиксируется при аудите доступа к объектам?
    A. Файл
    B. Каталог
    C. Учетная запись
    D. Ключ реестра

36. Какое действие не фиксируется при аудите системных событий?
    A. Запуск элементов системы безопасности
    B. Отключение элементов системы безопасности
    C. Присвоение привилегий пользователю
    D. Изменение системного времени

37. Какие события не фиксируются при аудите управления учетными записями?
    A. Создание учетной записи для пользователя
    B. Изменение пароля пользователя
    C. Назначение прав пользователю

38. Абсолютно защищенная система это -
    A. система, в которой существует только один администратор
    B. система, в которой существует разграничение доступа
    C. такая система не существует
    D. система, в которой каждый программный поток работает изолированно от других

39. Класс защищенности автоматизированной системы - это:
    A. Определенная совокупность требований по защите информации, предъявляемых к автоматизированной системе.
    B. определенное требование по защите информации, предъявляемых к персоналу автоматизированной системы.
    C. определенная совокупность требований по обработки информации, предъявляемых к автоматизированной системе.
    D. совокупность требований по обработки информации, предъявляемых к персоналу автоматизированной системе.

40 Механизм контроля целостности обеспечивает:

A. контроль учетных записей пользователей, прохождение ими процедур идентификации и аутентификации
B. разрешение или запрет работы с файлами, каталогами, устройствами, таблицами, полями и записями базы данных, сетевыми ресурсами
C. проверку неизменности контролируемых объектов в соответствии с заданным эталоном
D. фиксацию действий пользователей, доступа процессов к защищаемым ресурсам

41. Недостатками механизма контроля целостности в Windows является то, что (несколько вариантов):
A. Windows не проверяет файлы ядра операционной системы
B. Windows не проверяет файлы прикладных программ
C. Windows контролирует работоспособность, но не неизменяемость аппаратной среды
D. Контроль выполняется только при загрузке операционной системы

42. Контроль целостности файловых объектов решает задачи:
A. неизменности программной среды
B. неизменности аппаратной среды
C. неизменности списка пользователей
D. неизменности настроек BIOS

43. Как правило, контролируется целостность файлов следующих типов:
A. исполняемых и динамических библиотек
B. драйверов и системных файлов
C. графических файлов
D. текстовых документов

44. Для какого рода объектов следует осуществлять контроль целостности?
A. файлы с документами, обрабатываемые пользователями
B. графические файлы, содержащие черновые чертежи различных изделий
C. файлы, содержащие исполняемый код
D. файлы, содержащие тексты различного рода нормативных актов и нормативов

45. При доверенной загрузке ОС не выполняется:
A. процедуры идентификации и аутентификации пользователя
B. проверка целостности файловой системы
C. проверка целостности программной и аппаратной среды рабочего места
D. проверка целостности объектов загружаемой ОС.

46. При доверенной загрузке ОС:

A. ОС загружается только с жесткого диска
B. ОС загружается с внешнего носителя
C. ОС загружается только с сетевого диска

47. Укажите правильную последовательность этапов:

A. Передача управления модулю доверенной загрузки
B. Выполнение загрузочного сектора операционной системы
C. Выполнение микропрограммы BIOS

48. Какое из нижеперечисленного ПО не относится к средствам доверенной загрузки:

A. ПАК «Соболь»
B. Криптон ЗАМОК
C. Крипто Про
D. МДЗ Эшелон

49. Какое из нижеперечисленных средств доверенной загрузки имеет программное исполнение:

A. ПАК «Соболь»
B. Криптон ЗАМОК
C. Крипто Про
D. МДЗ Эшелон

50. Какие из нижеперечисленных средств доверенной загрузки имеют программно-аппаратное исполнение:

A. ПАК «Соболь»
B. Криптон ЗАМОК
C. Крипто Про
D. МДЗ Эшелон

51. Что из нижеперечисленного не может использоваться в качестве идентификатора:

A. iKey
B. eKey
C. eToken
D. ibutton

А2. Вопросы для устного опроса

1. Основные понятия и определения
2. Угрозы безопасности операционной системы (ОС)
3. Программно-технический уровень защиты информации в ОС
4. Классификация требований к системам защиты

5. Механизмы защиты ОС
6. Структура реестра Windows.
7. Основные ветви реестра.
8. Программные средства для работы с реестром.
9. Механизмы защиты реестра.
10. Импорт и экспорт ветвей реестра.
11. Субъекты и объекты доступа. Владение объектом.
12. Общие папки и разрешения NTFS. Специальные разрешения.
13. Маркер доступа. Дискреционные списки контроля доступа. Алгоритм проверки разрешений на доступ к объектам.
14. Управление доступом на основе Windows Rights Management Services
15. Мандатная модель доступа.
16. Дискреционная модель доступа.
17. Архитектура ОССН
18. Назначение ОССН
19. Области применения ОССН
20. Подсистема безопасности PARSEC
21. Варианты загрузки и регистрации в ОССН
22. Основные задачи администрирования ОССН
23. Назначение и функции модулей доверенной загрузки.
24. Особенности программных и программно-аппаратных средств МДЗ.
25. Средства идентификации в МДЗ.
26. МДЗ на российском рынке.
27. Журналы аудита
28. События, регистрируемые в журналах аудита
29. Политика аудита
30. Просмотр событий
31. Мягкая» защита (Soft Protection) каталогов

32. Подсистемы Windows File Protection и Windows Resource Protection. Методы защиты целостности. Кеширование данных. Особенности реализации в различных версиях ОС.
33. Архивация и восстановление данных. Теневые копии.
34. Управление дисковой памятью. Динамические диски. Обеспечение отказоустойчивости при использовании двух типа логических томов: зеркальный (RAID-1) и чередующийся с четностью (RAID-5).
35. Восстановление системы после сбоя. Последняя удачная конфигурация, Состояние системы, Автоматическое восстановление системы. Консоль восстановления. Особенности реализации в различных версиях ОС.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тематика рефератов

1. Безопасность информационных систем в нормативных документах
2. Классификация защищенности ОС по международным стандартам
3. Отечественные операционные системы
4. Особенности подсистемы информационной безопасности ParSec
5. Защита информации в мобильных операционных системах
6. Модель безопасности ОС семейства Window
7. Сравнение подсистем безопасности ОС семейств Window и Linux
8. Контроль доступа к объектам в ОС.
9. Ролевая модель доступа.
10. Механизмы защиты уровня ядра в ОС
11. Обеспечение безопасности серверных приложений ОС
12. Шифрованная файловая система EFS
13. Защита Active Directory
14. Системы защиты программного обеспечения

15. Средства защиты сетевого взаимодействия в ОС
16. Криптографическая защита сетевого взаимодействия
17. Файловые системы Window
18. Создание разделов и файловых систем ОС Linux. Монтирование файловых систем.
19. Журналируемая файловая система.
20. Реализация функций информационной безопасности в файловых системах.
21. Особенности настройки политики безопасности операционной системы специального назначения
22. Настройка политики безопасности сетевых ОС

В2. Тематика презентаций

1. Безопасность информационных систем в нормативных документах
2. Классификация защищенности ОС по международным стандартам
3. Отечественные операционные системы
4. Особенности подсистемы информационной безопасности ParSec
5. Защита информации в мобильных операционных системах
6. Модель безопасности ОС семейства Window
7. Сравнение подсистем безопасности ОС семейств Window и Linux
8. Контроль доступа к объектам в ОС.
9. Ролевая модель доступа.
10. Механизмы защиты уровня ядра в ОС
11. Обеспечение безопасности серверных приложений ОС
12. Шифрованная файловая система EFS
13. Защита Active Directory
14. Системы защиты программного обеспечения
15. Средства защиты сетевого взаимодействия в ОС
16. Криптографическая защита сетевого взаимодействия
17. Файловые системы Window

18. Создание разделов и файловых систем ОС Linux. Монтирование файловых систем.
19. Журналируемая файловая система.
20. Реализация функций информационной безопасности в файловых системах.
21. Особенности настройки политики безопасности операционной системы специального назначения
22. Настройка политики безопасности сетевых ОС

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

С.1. Лабораторная работа

Лабораторная работа «Работа с Реестром ОС Windows»

Задание 1. Изучение основных возможностей системного модуля «Редактор Реестра» ОС Windows на конкретных примерах

Задание 2. Изучение некоторых специальных возможностей Реестра ОС Windows в системном модуле «Редактор Реестра» на конкретных примерах.

Задание 3. Конфигурирование контекстного меню служебного программного средства «Мой компьютер» ОС Windows посредством применения редактора Реестра.

Задание 4. Конфигурирование ОС Windows с целью оптимизации ее работы и увеличения быстродействия.

Лабораторная работа «Настройка Политики учетных записей (Account Policy)»

Задание 1. Настройка минимальной длины пароля

Задание 2. Настройка и проверка дополнительных параметров политики учетных записей

Задание 3. Настройка Политики блокировки учетной записи (Account Lockout Policy)

Лабораторная работа «Настройка параметров безопасности»

Задание 1. Настройка параметра Учетные записи: переименование учетной записи гостя

Задание 2. Запрещение использования экрана приветствия

Задание 3. Настройка дополнительных параметров безопасности

Лабораторная работа «Управление дисковыми квотами»

Задание 1. Настройка параметров управления квотами

Задание 2. Запрещение дисковых квот

Лабораторная работа «Аудит ресурсов и событий»

Задание 1. Планирование политики аудита.

Задание 2. Настройка политики аудита.

Задание 3. Настройка аудита файлов.

Задание 4. Проверка правильности параметров политики аудита для файла AUDIT.

Задание 5. Просмотр журнала безопасности.

Задание 6. Управление журналом безопасности

Лабораторная работа «Управление дисковыми квотами»

Задание 1. Настройка параметров управления квотами

Задание 2. Запрещение дисковых квот

Лабораторная работа «Работа с учетными записями пользователей»

Задание 1. Создание, изменение и удаление локальных учетных записей пользователей

1. Создать новую локальную учетную запись пользователя с ограниченными правами и назначить для нее пароль с помощью категории Учетные записи пользователей (User Accounts).

2. Создадь консоль MMC с оснасткой Управление компьютером (Computer Management), а затем с ее помощью — еще две учетные записи.
3. Проверить одну из новых локальных учетных записей пользователей
4. Удалить локальную учетную запись пользователя с помощью категории Учетные записи пользователей (User Accounts).

Задание 2. Изменение параметров учетной записи пользователя

1. Изменение параметров учетной записи пользователя Задать и затем проверить действие параметра Запретить смену пароля пользователем (User Cannot Change Password).
2. Отключение учетной записи (Account Is Disabled)

Лабораторная работа «Управление группами»

Задание. Создание и администрирование локальной группы

1. Создать две локальные группы и во время создания добавить в них пользователей.
2. Добавить пользователя с помощью с помощью оснастки Управление компьютером (Computer Management) и
3. Добавить пользователя с помощью с помощью вкладки Членство в группах (Member Of) диалогового окна Свойства: *имя_учетной_записи.*
4. Удалить пользователя из группы и затем удалить одну из созданных локальных групп.

Лабораторная работа «Повышение безопасности с помощью EFS»

Задание 1. Шифрование файлов

Задание 2. Проверка зашифрованного файла

Задание 3. Расшифровка файлов и папок

Лабораторная работа «Сертификации в ОС семейства Microsoft Windows»

Задание 1. Установка ОС Windows Server

Задание 2. Настройка сервера сертификации

Лабораторная работа «Права доступа в Linux»

Задание 1. Ознакомиться с командами управления правами доступа и владения

Задание 2. Получить навыки работы с файловым менеджером Midnight Commander

Лабораторная работа «Работа с учетными записями и группами в ОССН»

Задание. Изучить особенности и освоить навыки администрирования локальных учетных записей пользователей и групп в ОССН с пользованием командной строки и графического интерфейса.

Лабораторная работа «Создание и настройка параметров мандатного управления доступом и мандатного контроля целостности»

Изучить и освоить администрирование основных параметров мандатного управления доступом в ОССН с применением графических утилит и командной строки.

Лабораторная работа «Мандатное управление доступом в файловой системе»

Изучить и освоить навыки администрирования мандатных управления доступом и контроля целостности в файловых системах и навыков использования утилиты «Управление политикой безопасности».

Лабораторная работа «Аутентификация пользователей в системе. Работа с модулями PAM»

Получить практический опыт настройки системы аутентификации в ОССН с использованием модулей PAM.

Лабораторная работа «Настройка сетевого взаимодействия»

Изучить принципы и порядок конфигурирования сетевого взаимодействия узлов АСЗИ на базе ОССН.

Освоить навыки решения задач управления сетевыми интерфейсами и протоколами, а также маршрутизацией пакетов.

Задание 6. Управление журналом безопасности

Лабораторная работа «Средства доверенной загрузки операционных систем»

Задание 1. Провести сравнительный анализ средств доверенной загрузки программного и программно-аппаратного типа.

Задание 2. Сравнение функциональных возможностей МДЗ «Эшелон», ПАК «Соболь», DallosLock.

Лабораторная работа «Архивация данных»

Задание 1. Выполнение задания архивации.

Задание 2. Создание и запуск автоматического задания архивации

Лабораторная работа «Восстановление данных»

Задание 1 Восстановление файлов из архива

Задание 2. Использование Мастера аварийного восстановления системы

Лабораторная работа «Архивация данных в Linux»

Задание: Ознакомиться с утилитами архивирования и сжатия в среде Linux.

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1.Перечень контрольных вопросов

1. Угрозы безопасности операционной системы. Типичные атаки на ОС. Классификация злоумышленников.
2. Понятие безопасности операционных систем. Классификация требований к системам защиты.
3. Понятие защищенной ОС. Общие принципы построения защищенных ОС. Механизмы защиты ОС

4. Реестр ОС Windows: понятие, структура, средства работы с реестром.
5. Назначение и возможности службы каталогов Active Directory.
6. Основные компоненты системы безопасности ОС.
7. Управление доступом в ОС. Модели управления доступом.
8. Подсистема аутентификации пользователей.
9. Аудит и обнаружение вторжений
10. Сетевая безопасность ОС
11. Основные понятия операционных систем специального назначения (ОССН)
12. Управление доступом в ОССН
13. Управление безопасностью в ОССН
14. Обеспечение целостности данных и систем
15. Виртуализация операционных систем
16. Доверенная загрузка ОС
17. Методы восстановления системы после сбоя: последняя удачная конфигурация, архивация состояния системы, точки восстановления, автоматическое восстановление системы, восстановление запуска, консоль восстановления.

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 дисциплине 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 шкала 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***
Устный опрос	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Подготовка реферата	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Подготовка презентации	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Тестирование	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение лабораторной работы	0-20	«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 дисциплине 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

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. Правильность ответов на вопросы.	Полно и аргументировано даны ответы по содержанию задания. Обнаружено понимание материала, может обосновать свои суждения, привести необходимые примеры. 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	«неудовле твори-тельно»		Студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

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.	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	«удовлетв орительно »		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	«неудовле твори-тельно»		Выполнено не более 53 % заданий предложенного теста, на поставленные вопросы ответ отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях).

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. Четкость изложения идеи реферата во время защиты.	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, четкое и последовательное выступление во время защиты.
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; выступление во время защиты требует дополнительных вопросов.
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 во время выступления.
0	«неудовлетвори-тельно»		Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы, не проведена защита реферата.

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»	4. Полнота выполнения; 5. Своевременность выполнения; 6. Четкость изложения идеи презентации во время защиты.	Выполнены все требования к подготовке презентации: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, четкое и последовательное выступление во время демонстрации.
3-4	«хорошо»		Основные требования к подготовке презентации выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем презентации; имеются упущения в оформлении; выступление во время демонстрации требует дополнительных вопросов.
1-2	«удовлетворительно»		Имеются существенные отступления от требований к презентации. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании презентации или при ответе на дополнительные вопросы во время выступления.
0	«неудовлетвори-тельно»		Тема презентации не раскрыта, обнаруживается существенное непонимание проблемы, не проведена демонстрация презентации.

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 выполнения лабораторных работ

Баллы	***Оценка***	***Показатели***	***Критерии***
18-20	«отлично»	1. Полнота выполнения задания лабораторной работы; 2. Своевременность выполнения задания лабораторной работы; 3. Самостоятельность решения.	Основные требования к выполнению задания лабораторной работы выполнены. Продемонстрировано умение анализировать ситуацию и находить оптимальное количества решений, умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для достижения поставленной цели
14-17	«хорошо»		Основные требования к выполнению задания лабораторной работы реализованы, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых решений
11-13	«удовлетворительно»		Имеются существенные отступления от выполнения лабораторной работы. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат
0-10	«неудовлетвори-тельно»		Шаги выполнения лабораторной работы не выполнены, обнаруживается существенное непонимание проблемы.

Лист актуализации оценочных материалов по дисциплине «Безопасность операционных систем»

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

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

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

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

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

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

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

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

Зав. кафедрой _____