Приложение 1

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

ОДОБРЕНО:
Методической комиссией по укрупненным группам специальностей и направлению подготовки 10.00.00- «Информационная безопасность»
Председатель МК
подпись ИОФ

УТВЕРЖДАЮ:
Декан, председатель совета факультета Компьютерных технологий, вычислительной техники и энергетики
подпись **Ш.А.Юсуфов** ИОФ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ Б.21

по дисциплине «Безопасность операционных систем» для контроля знаний обучающихся по специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем»

Фонд оценочных средств обсужден на заседании выпускающей кафедры ИБ «14.12» от 2018 года, протокол № 4.

Зав. кафедрой подпись Г.И.Качаева ИОФ

Оглавление

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ПК-26	способностью администрировать подсистему информационной безопасности автоматизированной системы	Должен знать – принципы построения и функционирования, примеры реализаций современных операционных систем; – функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами; – критерии оценки эффективности и надежности средств защиты операционных систем; – принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows.; Должен уметь – использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; – оценивать эффективность и надежность защиты операционных систем; – планировать политику безопасности операционных систем.; Должен владеть – профессиональной терминологией в области информационной безопасности; – навыками работы с операционными системами семейств UNIX и Windows, восстановление операционных систем после сбоев; – навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности; – навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.;
ПК-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	
ПК-14	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	
ПК-3	способностью проводить анализ защищенности автоматизированных систем	

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2. Реализация компетенций

2.1 Компетенция ПК-26

ПК-26: способностью администрировать подсистему информационной безопасности автоматизированной системы.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows	планировать политику безопасности операционных систем	навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;

	работы; • Лекции; • Самостоятельная работа;	работы; • Лекции; • Самостоятельная работа;	
Используемые средства оценивания	• Отчет по лабораторной работе; • Отчет по практике; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Отчет по практике; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Отчет по практике; • Зачет; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• знает в полном объеме принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;	• в полном объеме умеет планировать политику безопасности операционных систем;	• в полном объеме владеет навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;
Хорошо (базовый уровень)	• знает на продвинутом уровне принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;	• на продвинутом уровне умеет планировать политику безопасности операционных систем;	• на продвинутом уровне владеет навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;
Удовлетворительно (пороговый уровень)	• знает на базовом уровне принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;	• на базовом уровне умеет планировать политику безопасности операционных систем;	• на базовом уровне владеет навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных.

			локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;

2.2 Компетенция ПК-17

ПК-17: способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows	использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем	навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности
Виды занятий	• Интерактивные лабораторные занятия; • Интерактивные лекции; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Интерактивные практические занятия; • Практические занятия;	• Интерактивные лабораторные занятия; • Интерактивные лекции; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Интерактивные практические занятия; • Практические занятия;	• Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа; • Интерактивные практические занятия;
Используемые средства оценивания	• Отчет по лабораторной работе; • Отчет по практике; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Отчет по практике; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Отчет по практике; • Зачет; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично	• знает в полном	• в полном объеме	• в полном объеме

(высокий уровень)	объеме принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;	умеет использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;	владеет навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;
Хорошо (базовый уровень)	• знает на продвинутом уровне принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;	• на продвинутом уровне умеет использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;	• на продвинутом уровне владеет навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;
Удовлетворительно (пороговый уровень)	• знает на базовом уровне принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;	• на базовом уровне умеет использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;	• на базовом уровне владеет навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;

2.3 Компетенция ПК-14

ПК-14: способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 7.

Таблица 7 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть

Содержание этапов	критерии оценки эффективности и надежности средств защиты операционных систем	оценивать эффективность и надежность защиты операционных систем	навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности
Виды занятий	• Интерактивные лабораторные занятия; • Интерактивные лекции; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Интерактивные практические занятия; • Практические занятия;	• Интерактивные лабораторные занятия; • Интерактивные лекции; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Интерактивные практические занятия; • Практические занятия;	• Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа; • Интерактивные практические занятия;
Используемые средства оценивания	• Отчет по лабораторной работе; • Отчет по практике; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Отчет по практике; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Отчет по практике; • Зачет; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 8.

Таблица 8 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• знает в полном объеме каковы критерии оценки эффективности и надежности средств защиты операционных систем;	• в полном объеме умеет оценивать эффективность и надежность защиты операционных систем;	• в полном объеме владеет навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности;
Хорошо (базовый уровень)	• знает на продвинутом уровне каковы критерии оценки эффективности и надежности средств защиты операционных систем;	• на продвинутом уровне умеет оценивать эффективность и надежность защиты операционных систем;	• на продвинутом уровне владеет навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной

			безопасности;
Удовлетворительно (пороговый уровень)	• знает на базовом уровне каковы критерии оценки эффективности и надежности средств защиты операционных систем;	• на базовом уровне умеет оценивать эффективность и надежность защиты операционных систем;	• на базовом уровне владеет навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности;

2.4 Компетенция ПК-3

ПК-3: способностью проводить анализ защищенности автоматизированных систем.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 9.

Таблица 9 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	принципы построения и функционирования, примеры реализаций современных операционных систем	оценивать эффективность и надежность защиты операционных систем	навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Опрос на занятиях; • Отчет по практике; • Зачет; • Экзамен;	• Контрольная работа; • Опрос на занятиях; • Отчет по практике; • Зачет; • Экзамен;	• Отчет по практике; • Зачет; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 10.

Таблица 10 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично	• знает в полном	• в полном объеме	• в полном объеме

(высокий уровень)	объеме принципы построения и функционирования, примеры реализаций современных операционных систем;	умеет оценивать эффективность и надежность защиты операционных систем;	владеет навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности;
Хорошо (базовый уровень)	• знает на продвинутом уровне принципы построения и функционирования, примеры реализаций современных операционных систем;	• на продвинутом уровне умеет оценивать эффективность и надежность защиты операционных систем;	• на продвинутом уровне владеет навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности;
Удовлетворительно (пороговый уровень)	• знает на базовом уровне принципы построения и функционирования, примеры реализаций современных операционных систем;	• на базовом уровне умеет оценивать эффективность и надежность защиты операционных систем;	• на базовом уровне владеет навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности;

3. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

3.1 Вопросы для входной контрольной работы

1. Дать определение и характеристику основных режимов работы, дисциплин и режимов обслуживания заявок в вычислительных системах.
2. Дать определение и характеристику классов программных средств.
3. Изложить классификацию ОС.
4. Охарактеризовать основные принципы построения ОС.
5. Перечислить виды интерфейсов ОС. Охарактеризовать пакетную технологию как интерфейс. Дать описание интерфейса командной строки.
6. Дать описание графических интерфейсов. В каких ОС они применяются?
7. Охарактеризовать речевую технологию как интерфейс.
8. Охарактеризовать биометрическую технологию как интерфейс.
9. Охарактеризовать семантический интерфейс.

3.2Контрольные работы по проверке текущих знаний студентов

Контрольная работа №1

1. Основные понятия и положения защиты информации в информационно-вычислительных системах.
2. Предмет защиты информации.
3. Основные положения безопасности информационных систем.

4. Основные принципы обеспечения информационной безопасности в информационных системах
5. Угрозы безопасности информации в информационно-вычислительных системах
6. Анализ угроз информационной безопасности.

Контрольная работа №2

1. Методы обеспечения информационной безопасности.
2. Классификация злоумышленников
3. Основные направления и методы реализации угроз информационной безопасности.
4. Угрозы безопасности ОС.
5. Классификация угроз безопасности ОС. Наиболее распространенные угрозы
6. Программно-технический уровень информационной безопасности
7. Основные понятия программно-технического уровня информационной безопасности.
8. Требования к защите компьютерной информации. Классификация требований к системам защиты.
9. Формализованные требования к защите информации от НСД.

Контрольная работа №3

1. Общие подходы к построению систем защиты компьютерной информации.
2. Различия требований и основополагающих механизмов защиты от НСД
3. Требования к защите ОС.
4. Понятие защищенной ОС.
5. Подходы к организации защиты ОС и их недостатки.
6. Этапы построения защиты. Административные меры защиты.
7. Стандарты безопасности ОС
8. Анализ выполнения современными ОС формализованных требований к защите информации от НСД.
9. Анализ существующей статистики угроз для современных универсальных ОС
10. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа.

3.3 Вопросы к зачету по дисциплине «Безопасность операционных систем»

1. Основные понятия и положения защиты информации в информационно-вычислительных системах.
2. Основные положения безопасности информационных систем.
3. Угрозы безопасности информации в информационно-вычислительных системах
4. Анализ угроз информационной безопасности.
10. Методы обеспечения информационной безопасности.
11. Угрозы безопасности ОС.
12. Классификация угроз безопасности ОС. Наиболее распространенные угрозы
13. Программно-технический уровень информационной безопасности
14. Основные понятия программно-технического уровня информационной безопасности.
11. Различия требований и основополагающих механизмов защиты от НСД
12. Требования к защите ОС.
13. Понятие защищенной ОС.
14. Подходы к организации защиты ОС и их недостатки.
15. Этапы построения защиты. Административные меры защиты.
16. Стандарты безопасности ОС
17. Анализ существующей статистики угроз для современных универсальных ОС

3.4 Вопросы для входной контрольной работы

1. Основные положения безопасности информационных систем.
2. Анализ угроз информационной безопасности.
3. Угрозы безопасности ОС.
4. Классификация угроз безопасности ОС. Наиболее распространенные угрозы

5. Основные понятия программно-технического уровня информационной безопасности.
6. Различия требований и основополагающих механизмов защиты от НСД
7. Требования к защите ОС.
8. Понятие защищенной ОС.
9. Подходы к организации защиты ОС и их недостатки.
10. Этапы построения защиты. Административные меры защиты.
11. Стандарты безопасности ОС

3.5 Контрольные работы по проверке текущих знаний студентов

Контрольная работа №4

1. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС
2. Понятия идентификации и аутентификации пользователей.
3. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей.
4. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя.
5. Примеры реализации идентификации и аутентификации в современных ОС.
6. POSIX-совместимые операционные системы. Особенности архитектуры. История развития. Общая характеристика языка командного интерпретатора POSIX-совместимых ОС.
7. Переменные языка командного интерпретатора POSIX-совместимых ОС и их использование. Встроенные переменные

Контрольная работа №5

1. Управление порядком выполнения действий в языке командного интерпретатора POSIX-совместимых ОС. Команды для работы с файлами, каталогами, процессами, перенаправление ввода-вывода.
2. Отладка сценариев. Назначение и функции систем выполнения сценариев Windows. Объектные модели и языки систем выполнения сценариев ОС Windows.
3. Удаленное выполнение сценариев ОС Windows. Цифровая подпись сценариев в ОС Windows.
4. Классификация угроз безопасности ОС. Наиболее распространенные угрозы.
5. Понятие защищенной ОС.
6. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.
7. Стандарты безопасности ОС. Виртуальные машины. Изоляция процессов и пользователей.

Контрольная работа №6

1. Политики безопасности в ОС Windows
2. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа.
3. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС.
4. Понятия идентификации, аутентификации и учета. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей
5. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя. Примеры реализации идентификации, аутентификации и учета в современных ОС.
6. Необходимость аудита. Требования к подсистеме аудита.
7. Централизованный аудит. Штатный аудит в ОС Windows.
8. Реализации аудита в современных ОС.

3.6 Вопросы к экзамену по дисциплине «Безопасность операционных систем»

1. Основные понятия и положения защиты информации в информационно-вычислительных системах.
2. Предмет защиты информации.
3. Основные положения безопасности информационных систем.
4. Основные принципы обеспечения информационной безопасности в информационных системах
5. Угрозы безопасности информации в информационно-вычислительных системах
6. Анализ угроз информационной безопасности.
7. Методы обеспечения информационной безопасности.
8. Классификация злоумышленников
9. Основные направления и методы реализации угроз информационной безопасности.
10. Угрозы безопасности ОС.
11. 11 .Классификация угроз безопасности ОС. Наиболее распространенные угрозы
12. Программно-технический уровень информационной безопасности
13. Основные понятия программно-технического уровня информационной безопасности.
14. Требования к защите компьютерной информации. Классификация требований к системам защиты.
15. Формализованные требования к защите информации от НСД.
16. Общие подходы к построению систем защиты компьютерной
17. информации.
18. Различия требований и основополагающих механизмов защиты от НСД
19. Требования к защите ОС.
20. Понятие защищенной ОС.
21. Подходы к организации защиты ОС и их недостатки.
22. Этапы построения защиты. Административные меры защиты.
23. Стандарты безопасности ОС
24. Анализ выполнения современными ОС формализованных требований к защите информации от НСД.
25. Анализ существующей статистики угроз для современных универсальных ОС
26. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС
27. Понятия идентификации и аутентификации пользователей.
28. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей.
29. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя.
30. Примеры реализации идентификации и аутентификации в современных ОС.
31. P081X-совместимые операционные системы. Особенности архитектуры. История развития. Общая характеристика языка командного интерпретатора POSIX-совместимых ОС.
32. Переменные языка командного интерпретатора POSIX-совместимых ОС и их использование. Встроенные переменные
33. Управление порядком выполнения действий в языке командного интерпретатора POSIX-совместимых ОС. Команды для работы с файлами, каталогами, процессами, перенаправление ввода-вывода.
34. 34.Отладка сценариев. Назначение и функции систем выполнения сценариев Windows. Объектные модели и языки систем выполнения сценариев ОС Windows.
35. Удаленное выполнение сценариев ОС Windows. Цифровая подпись сценариев в ОС Windows.
36. Классификация угроз безопасности ОС. Наиболее распространенные угрозы.
37. Понятие защищенной ОС.
38. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.
39. Стандарты безопасности ОС. Виртуальные машины. Изоляция процессов и пользователей.

40. Политики безопасности в ОС Windows
41. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя. Примеры реализации идентификации, аутентификации и учета в современных ОС.
42. Централизованный аудит. Штатный аудит в ОС Windows.
43. Реализации аудита в современных ОС.

3.7 Вопросы для контроля остаточных знаний по дисциплине «Безопасность операционных систем»

1. Основные понятия и положения защиты информации в информационно-вычислительных системах.
2. Основные положения безопасности информационных систем.
3. Основные принципы обеспечения информационной безопасности в информационных системах
4. Основные направления и методы реализации угроз информационной безопасности.
5. Основные понятия программно-технического уровня информационной безопасности.
6. Методы обеспечения информационной безопасности.
7. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа.
8. Понятие защищенной ОС.
9. Стандарты безопасности ОС.
10. Подходы к организации защиты ОС и их недостатки.
11. Общие подходы к построению систем защиты компьютерной информации.
12. Понятия идентификации и аутентификации пользователей.
13. Политики безопасности в ОС Windows
14. Реализации аудита в современных ОС

4. Учебно-методическое и информационное обеспечение дисциплины «Безопасность операционных систем»

№п\п	Видызаня тий	Комплект необходимой учебной литературы по дисциплине	Автор	Издат. и год изд.	Количество пособий, учебников и прочей литературы	
					В библ.	На каф.
Основная литература						
1.	ЛЗ, ЛБ, СРС	Метода и средства защиты информации в компьютерных системах: учебное пособие для студ. высш. учеб.заведений	Хорев П.Б.	М: Издательский центр «Академия», 2007. – 256с	1	1
2.	ЛЗ, ЛБ, СРС	Основы операционных систем [Электронный ресурс]	К. А. Коньков, В. Е. Карпов.	М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 346 c. — 2227-8397	http://www.iprbookshop.ru/73693.html	
3.	ЛЗ, ЛБ, СРС	Средства безопасности операционной системы WindowsServer 2008 [Электронный ресурс]	Глотина, И. М.	Саратов: Вузовское образование, 2018. — 141 c. — 978-5-4487-0136-8.	http://www.iprbookshop.ru/72538.html	
4.	ЛЗ, ЛБ, СРС	Средства безопасности операционной системы WindowsServer 2008 [Электронный ресурс]	Глотина, И. М.	Саратов : Вузовское образование, 2018. — 141 c. — 978-5-4487-0136-8.	http://www.iprbookshop.ru/72538.html	
5.	ЛЗ, ЛБ, СРС	Средства безопасности операционной системы ROSA Linux [Электронный ресурс]	Ложников, П. С.	Омск : Омский государственный технический университет, 2017. — 94 c. — 978-5-8149-2502-2	http://www.iprbookshop.ru/78474.html	
6.	ЛЗ, ЛБ, СРС	Сетевые операционные системы : учебник для вузов -	В.Г. Олифер, Н.А. Олифер.	СПб : Питер, 2005. - 544 с. : ил	10	1
7.	ЛЗ, ЛБ, СРС	Операционные системы: учеб.	Г.Х. Ирзаев	МО и Н РФ ГОУ ВПО "ДГТУ", Кафедра "ИСЭ". - Махачкала : Формат, 2011.	10	1
Дополнительная литература						
8.	ЛЗ, ЛБ, СРС	Операционная система MicrosoftWindows XP. Русская версия [Электронный ресурс]	Ай Пи Эр Медиа,	М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2019. — 374 c. — 978-5-4486-0514-7.	http://www.iprbookshop.ru/79715.html	
9.	ЛЗ, ЛБ, СРС	Операционные системы. Часть 1 [Электронный ресурс] : учебное пособие	Гриценко, Ю. Б.	Томск: Томский государственный университет систем управления и радиоэлектроники, 2009. — 187 c. — 2227-8397	http://www.iprbookshop.ru/13952.html	
10.	ЛЗ, ЛБ, СРС	Операционные системы. Часть 2 [Электронный ресурс] : учебное пособие	Гриценко, Ю. Б.	Томск: Томский государственный университет систем управления и радиоэлектроники, 2009. — 230 c. — 2227-8397	http://www.iprbookshop.ru/13953.html	

5. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий на факультете имеется комплект технических средств обучения в составе:

- интерактивная доска;

– переносной компьютер (в конфигурации не хуже: процессор IntelCore 2 Duo, 2 Гбайта ОЗУ, 500 Гбайт НЖМД);

– проектор (разрешение не менее 1280x1024);

Для проведения лабораторных занятий имеется компьютерный класс, оборудованный компьютерами с установленным программным обеспечением, предусмотренным программой дисциплины.