Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю) Безопасность операционных систем

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Специализация №4
Безопасность автоматизированных систем критически важных объектов

Присваиваемая квалификация (степень)
Специалист по защите информации

Форма обучения
Очная

Год набора 2025

Челябинск, 2025 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность: 10.05.03 Информационная безопасность автоматизированных систем
Специализация: Безопасность автоматизированных систем критически важных объектов
Дисциплина: Безопасность операционных систем
Семестр: 6
Форма промежуточной аттестации: экзамен
Система оценивания: оценивание результатов осуществляется в рамках 5-балльной системы

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Безопасность операционных систем» направлено на формирование следующих компетенций:

Коды компетенции (по ФГОС)	Содержание компетенций согласно ФГОС	Индикаторы достижения компетенций согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
ОПК-11	Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ОПК-11.1. Имеет представление о компонентах систем защиты информации автоматизированных систем. ОПК-11.2. Имеет практический опыт разрабатывать компоненты систем защиты информации автоматизированных систем.	Для достижения индикатора ОПК-11.1: Знать о компонентах систем защиты информации автоматизированных систем (основные определения и положения безопасности ОС, основные защитные механизмы клиентских ОС). Для достижения индикатора ОПК-11.2: Уметь разрабатывать компоненты систем защиты информации автоматизированных систем (осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации). Для достижения индикатора ОПК-11.2: Владеть навыками разработки компонентов систем защиты информации автоматизированных систем.
ОПК-12	Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12.1. Обладает базовыми знаниями в области безопасности вычислительных сетей, операционных систем и баз данных. ОПК-12.2. Демонстрирует умения применять при разработке автоматизированных систем знания в области безопасности вычислительных сетей, операционных систем и баз данных.	Для достижения индикатора ОПК-12.1: Знать базовые понятия в области безопасности операционных систем. Для достижения индикатора ОПК-12.2: Уметь применять при разработке автоматизированных систем знания в области безопасности операционных систем. Для достижения индикатора ОПК-12.2: Владеть навыками применения при разработке автоматизированных систем знания в области безопасности операционных систем.
ОПК-13	Способен	ОПК-13.1. Обладает	Для достижения индикатора ОПК-13.1:

	организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	знаниями о диагностике, тестировании и анализе уязвимостей систем защиты информации автоматизированных систем. ОПК-13.2. Демонстрирует умения организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем. ОПК-13.3. Имеет практический опыт проводить анализ уязвимостей систем защиты информации автоматизированных систем.	Знать о диагностике, тестировании и анализе уязвимостей систем защиты информации автоматизированных систем (программно-аппаратные средства обеспечения информационной безопасности в типовых операционных систем, в системах управления базами данных, вычислительных сетях). Для достижения индикатора ОПК-13.2: Уметь организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем (оценивать угрозы безопасности клиентским ОС, осуществлять проверку защищенности клиентских ОС, осуществлять проверку защищенности серверных ОС). Для достижения индикатора ОПК-13.3: Владеть навыками проведения анализа уязвимостей систем защиты информации автоматизированных систем (навыками настройки политики безопасности и учетных записей ОС, оценки степени защищенности клиентских ОС, навыками оценки степени безопасности ОС, навыками администрирования протокольных средств обеспечения безопасности ОС, навыками администрирования прав пользователей и аудита доступа к ресурсам ОС).

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1 Виды оценочных средств

№ п/п	Код компетенции	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1.	ОПК-11 ОПК-12 ОПК-13	Подсистема защиты информации в ОС UNIX	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№1-6)
		Подсистема Защиты информации в ОС Windows	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№7-10)
		Защита информации при интеграции UNIX и Windows	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№11-13)
		Программно-аппаратные методы и средства ограничения	Собеседование и отчеты по	Вопросы к экзамену (№14-16)

		доступа к ресурсам ПЭВМ	лабораторным работам.	
		Подсистема защиты информации в ОС UNIX	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№17-19)
		Инфраструктура открытых ключей PKI	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№20-23)
		Службы сертификации в ОС Windows	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№24)
		Служба управления правами ADRMS	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№25)
		Безопасность ОС Windows на серверном уровне	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№26-29)
		Шифрование IPsec в ОС Windows	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№30-32)
		Сервер сетевых политик, защита и маршрутизациия сетевого доступа и дистанционный доступ	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№33-39)

3.2 Содержание оценочных средств

Темы лабораторных работ:

1. Создание бюджетов пользователя; Использование списков доступа; аудит в ОС Windows, UNIX.
2. Оценка защищенности заданной конфигурации Windows: файловая система, реестр, список пользователей, политика безопасности в области паролей
3. Интеграция сетей Microsoft и UNIX с использованием сервера Samba
4. Изучение средств защиты сетевого взаимодействия Unix
5. Поиск программных закладок в заданной консультации Windows
6. Использование возможностей файловой системы ОС Windows для шифрования файлов
7. Подсистема защиты информации в ОС UNIX. Основы информационной безопасности. Концепции безопасности UNIX. Настройка системы безопасности
8. Изучение инфраструктуры открытых ключей
9. Изучение создания смарт-карт в инфраструктуре открытых ключей

10. Изучение защиты конфигурации ADCS
11. Создание репозитория сертификатов и восстановление ЦС
12. Изучение службы управление правами. Изучение основных настроек службы управления правами
13. Изучение физической безопасности сервера. Изучение дополнительных мер безопасности. Изучение службы обновления Windows Server
14. Изучение компонентов NAP. Изучение протокола RADIUS
15. Развертывание и внедрение виртуальной частной сети
16. Внедрение параметров политики с помощью сервера сетевых политик

Критерии оценивания лабораторной работы:

В процессе выполнения лабораторной работы каждый студент составляет индивидуальный отчет, который включает расчетную часть, а также аналитическую часть и выводы. По подготовленному отчету проводится собеседование.

Лабораторная работа засчитывается студенту, если он представил правильно оформленный отчет, владеет методикой обработки данных; усвоил теоретический материал по данной теме (последовательно, грамотно и логически стройно его излагает, уверенно отвечает на вопросы). Допускаются несущественные неточности в оформлении и ответах на вопросы.

Лабораторная работа не засчитывается студенту в случаях: наличия ошибок в расчетах, неправильного оформления отчета, искажающего смысл задания, существенных ошибок при ответах на вопросы.

Вопросы к экзамену:

1. Основные компоненты подсистем защиты UNIX.
2. Файловая система – как основа подсистемы защиты.
3. Права доступа к элементам файловой системы.
4. Управление процессами.
5. Создание и удаление бюджетов пользователей.
6. Основные проблемы с безопасностью и возможные решения в UNIX-подобных системах.
7. Основные компоненты подсистем защиты Windows.
8. Политики.
9. Понятие домена.
10. Особенности установления доверительных отношений.
11. Основы взаимодействия элементов гетерогенных сетей.
12. Шлюзы NFS. SMB в UNIX.
13. Использование сервера Samba для разделения доступа к сетевым ресурсам в домене Windows.
14. Методы и средства ограничения доступа к компонентам ПЭВМ.
15. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
16. Методы и средства хранения ключевой информации.
17. Основы информационной безопасности.
18. Концепции безопасности UNIX.
19. Настройка системы безопасности.
20. Основные компоненты PKI.
21. Функции удостоверяющего и регистрационного центров, репозитория, архива

сертификатов, серверных компонентов PKI.
22. Краткая характеристика сервисов PKI и сервисов, базирующихся на PKI.
23. Криптографические и вспомогательные сервисы, сервисы управления сертификатами.
24. Службы сертификации в ОС Windows.
25. Служба управления правам ADRMS.
26. Обеспечения физической безопасности WindowsServer.
27. Создание входящих и исходящих правил для брандмауэра.
28. Доступ к системе с помощью смарт-карт.
29. Дополнительные меры безопасности (Защита с помощью резервного копирования, работа со службой обновления).
30. Шифрование IPsec в WindowsServer 2008R2.
31. Принципы работы IPsec.
32. Основные возможности IPsec. NATTraversal в IPsec.
33. Защита сетевого доступа (NAP) в WindowsServer 2008R2.
34. Причины развертывания NAP.
35. Обзор компонентов NAP.
36. Концепция NPS.
37. Туннели VPN.
38. Протоколы PPTP, L2TP.
39. Активизация VPN на сервере RRAS

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

Студент допускается к экзамену по дисциплине в случае выполнения им учебного плана по дисциплине: выполненных и защищенных работ. В случае наличия учебной задолженности студент отрабатывает пропущенные занятия в форме, предложенной преподавателем и представленной в настоящей программе.

Экзамен проводится по билетам в устной форме. При проведении экзамена экзаменуемый выбирает билет в случайном порядке. Экзаменатору предоставляется право по ходу экзамена задавать экзаменуемому уточняющие и дополнительные вопросы. Время подготовки студента для устного ответа на экзамене должно составлять не менее 40 минут, время ответа экзаменуемого – не более 20 минут. При подготовке и ответе на вопросы билета экзаменуемый должен вести необходимые записи в листе устного ответа, который по окончании экзамена подписывается студентом, сдаётся экзаменатору и сохраняется им до окончания экзаменационной сессии. Студент, испытавший затруднения при подготовке к ответу по выбранному билету, вправе выбрать второй билет с продлением времени на подготовку. При этом окончательная оценка студента снижается на один балл. Выбор студентом третьего билета не допускается.

Проявленные студентом в ходе экзамена знания оцениваются оценками «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств

Критерии оценивания ответа (устного опроса) на экзамене:

Оценка «отлично» выставляется:

Дан полный, развернутый ответ на поставленный вопрос, показана совокупность

осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знания по предмету демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком с использованием современной терминологии. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.

Оценка «хорошо» выставляется:

Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком с использованием современной терминологии. Могут быть допущены некоторые неточности или незначительные ошибки, исправленные студентом с помощью преподавателя.

Оценка «удовлетворительно» выставляется:

Дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.

Оценка «неудовлетворительно» выставляется:

1) Ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь обсуждаемого вопроса по билету с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента.

2) Ответ на вопрос полностью отсутствует.

3) Отказ от ответа.

Особенности проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обозначены в рабочей программе дисциплины (модуля).

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

1. Высокий уровень сформированности компетенций соответствует оценке «отлично».
2. Средний уровень сформированности компетенций соответствует оценке «хорошо».
3. Базовый уровень сформированности компетенций соответствует оценке «удовлетворительно».
4. Низкий уровень сформированности компетенций соответствует оценке «неудовлетворительно».

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:
Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом физического факультета

Протокол заседания № 05 от 06.02.2025

Председатель Ученого совета
физического факультета согласовано М.А. Загребин

Заседанием кафедры радиофизики и электроники

Протокол заседания № 07 от 04.02.2025

Заведующий кафедрой согласовано А.В. Бутаков

Автор (составитель) М.А. Загребин

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1