МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. декана факультета
математики и компьютерных
наук имени профессора Н.И. Червякова
Гробова Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
«Безопасность операционных систем»

Специальность	Информационная безопасность автоматизированных систем
Направленность (профиль)	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	7

Предисловие

1. 1. Назначение: проведение текущего контроля успеваемости и промежуточной аттестации по дисциплине «Безопасность операционных систем». Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информации о ходе и качестве освоения компетенций, а также стимулирование регулярной целенаправленной работы студентов. Для формирования определенного уровня компетенций.

2. ФОС является приложением к программе дисциплины «Безопасность операционных систем».

3. Разработчики: Ляхов А.В., - доцент кафедры вычислительной математики и кибернетики

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:
Бабенко М. Г.– зав. кафедрой вычислительной математики и кибернетики

Члены комиссии:
Пелешенко В. С. – доцент кафедры вычислительной математики и кибернетики
Пелешенко Т. А. – доцент кафедры вычислительной математики и кибернетики

Представитель организации-работодателя: Корниенко С.А. начальник управления филиала ФГУП «Главный радиочастотный центр» в Южном и Северо-Кавказском федеральных округах.
Экспертное заключение: фонд оценочных средств соответствует образовательной программе по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» и рекомендуется для проведения текущего контроля успеваемости и промежуточной аттестации студентов.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

1. Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания

Компетенция (ии), индикатор (ы)	Уровни сформированности компетенци(ий)			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	**Минимальный уровень (удовлетворительно) 3 балла**	**Средний уровень (хорошо) 4 балла**	**Высокий уровень (отлично) 5 баллов**
Компетенция: **ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем**				
Результаты обучения по дисциплине: *Индикатор:* **ИД-1$_{ОПК-12}$** Осуществляет анализ и диагностику операционных систем; выбирает оптимальные критерии оценки эффективности и надежности средств защиты операционных систем; понимает базовые принципы организации и структуру подсистем защиты операционных систем семейства UNIX и Windows; анализирует функции операционных систем, основные	Не предоставляет отчет, с пояснением в котором описывает операционные системы; критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейства UNIX и Windows; функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами.	Предоставляет неполный отчет с пояснением в котором описывает операционные системы; критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейства UNIX и Windows; функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью,	Предоставляет отчет, с полным пояснением в котором описывает операционные системы; критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейства UNIX и Windows; функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами.	Предоставляет детальный отчет с полным пояснением в котором описывает операционные системы; критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейства UNIX и Windows; функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами.

концепции управления процессорами, памятью, вспомогательной памятью, устройствами		устройствами.		
Результаты обучения по дисциплине: *Индикатор:* **ИД-2опк-12** Использует средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивает эффективность и надёжность защиты операционных систем; планирует политику безопасности операционных систем.	Не предоставляет отчет, где демонстрирует способность использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем.	Предоставляет неполный отчет где демонстрирует способность использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем.	Предоставляет отчет, где демонстрирует способность использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем.	Предоставляет детальный отчет, где демонстрирует способность использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем.
Результаты обучения по дисциплине: *Индикатор:* **ИД-3опк-12** Способен применять знания в области	Не предоставляет отчет, где демонстрирует способность применять знания в области безопасности	Предоставляет неполный отчет где демонстрирует способность применять знания в области	Предоставляет отчет, где демонстрирует способность применять знания в области безопасности операционных	Предоставляет детальный отчет, где демонстрирует способность применять знания в области безопасности

безопасности операционных систем при разработке автоматизированных систем.	операционных систем при разработке автоматизированных систем.	безопасности операционных систем при разработке автоматизированных систем.	систем при разработке автоматизированных систем.	операционных систем при разработке автоматизированных систем.
Компетенция: **ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем**				
Результаты обучения по дисциплине: *Индикатор:* **ИД-1опк-13** Оценивает вероятность возникновения потенциальных угроз информационной безопасности предприятия (организации); использует методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации; определяет основные действия сотрудника информационной безопасност	Не предоставляет отчет в котором демонстрирует основные угрозы информационной безопасности предприятия (организации), а так же методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации и описывает основные действия сотрудника информационной безопасности предприятия (организации) при возникновении либо обнаружении следов компьютерных преступлений с	Предоставляет неполный отчет с неполным пояснением в котором демонстрирует основные угрозы информационной безопасности предприятия (организации), а так же методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации и описывает основные действия сотрудника информационной безопасности предприятия (организации) при возникновении либо обнаружении	Предоставляет отчет с пояснением в котором демонстрирует основные угрозы информационной безопасности предприятия (организации), а так же методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации и описывает основные действия сотрудника информационной безопасности предприятия (организации) при возникновении либо обнаружении следов компьютерных	Предоставляет детальный отчет с полным пояснением в котором демонстрирует основные угрозы информационной безопасности предприятия (организации), а так же методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации и описывает основные действия сотрудника информационной безопасности предприятия (организации) при возникновении либо обнаружении следов компьютерных преступлений с использованием методов

и предприятия (организации) при возникновении либо обнаружении следов компьютерных преступлений; использует методы расследования компьютерных преступлений и инцидентов.	использование м методов расследования компьютерных преступлений и инцидентов.	следов компьютерных преступлений использованием методов расследования компьютерных преступлений и инцидентов.	преступлений с использование м методов расследования компьютерных преступлений и инцидентов	расследования компьютерных преступлений и инцидентов
Результаты обучения по дисциплине: *Индикатор:* **ИД-2опк-13** Проводит диагностику компьютерной системы на обнаружение программно-аппаратных средств совершения киберпреступлений; выявляет следы совершения компьютерных преступлений и проведению оценки защищенности	Не предоставляет отчет в котором демонстрирует свою способность проводить диагностику компьютерной системы на обнаружение программно-аппаратных средств совершения киберпреступленийи выявлять следы совершения компьютерных преступлений и проведению оценки защищенности компьютерной системы на защиту информации.	Предоставляет неполный отчет в котором демонстрирует свою способность проводить диагностику компьютерной системы на обнаружение программно-аппаратных средств совершения киберпреступленийи выявлять следы совершения компьютерных преступлений и проведению оценки защищенности компьютерной системы на	Предоставляет отчет в котором демонстрирует свою способность проводить диагностику компьютерной системы на обнаружение программно-аппаратных средств совершения киберпреступленийи выявлять следы совершения компьютерных преступлений и проведению оценки защищенности компьютерной системы на защиту информации.	Предоставляет детальный отчет в котором демонстрирует свою способность проводить диагностику компьютерной системы на обнаружение программно-аппаратных средств совершения киберпреступлений и выявлять следы совершения компьютерных преступлений и проведению оценки защищенности компьютерной системы на защиту информации.

компьютерной системы на защиту информации.		защиту информации.		
Результаты обучения по дисциплине: *Индикатор:* **ИД-З$_{ОПК-13}$** Способен организовывать и проводить диагностику и тестировать системы защиты информации автоматизированных систем, проводит анализ уязвимостей систем защиты информации автоматизированных систем при расследовании компьютерных преступлений и инцидентов.	Не предоставляет отчет в котором показывает свою способность организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем при расследовании компьютерных преступлений и инцидентов.	Предоставляет неполный отчет в котором показывает свою способность организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем при расследовании компьютерных преступлений и инцидентов.	Предоставляет отчет в котором показывает свою способность организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем при расследовании компьютерных преступлений и инцидентов	Предоставляет детальный отчет в котором показывает свою способность организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем при расследовании компьютерных преступлений и инцидентов.

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры - в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» в актуальной редакции.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Семестр 7	
1.	b	Что такое "доверенная вычислительная база" (TCB) в ОС? a) Все установленные приложения b) Совокупность компонентов, отвечающих за безопасность c) Журнал системных событий d) Файл подкачки	ОПК-12, ОПК - 13
2.	b	Какой принцип безопасности предполагает минимальные привилегии для пользователей? a) Полный запрет b) Принцип наименьших привилегий c) Свободный доступ d) Автоматическое повышение прав	ОПК-12, ОПК -13
3.	b	Что обеспечивает механизм "песочницы" (sandbox)? a) Ускорение работы программ b) Изоляцию потенциально опасных процессов c) Автоматическое обновление системы d) Шифрование файлов	ОПК-12, ОПК -13
4.	c	Какой механизм НЕ относится к методам аутентификации? a) Пароли b) Биометрия c) Сетевые фильтры d) Аппаратные токены	ОПК-12, ОПК -13
5.	a	Что такое ACL (Access Control List)? a) Список разрешений для объектов системы b) Журнал ошибок c) Перечень установленных программ d) Список сетевых подключений	ОПК-12, ОПК -13
6.	c	Какой тип контроля доступа использует метки безопасности?	ОПК-12, ОПК -13

		a) Дискреционный (DAC) b) Ролевой (RBAC) c) Мандатный (MAC) d) Атрибутный (ABAC)	
7.	a	Для чего используется технология ASLR? a) Для защиты от атак переполнения буфера b) Для ускорения загрузки ОС c) Для сжатия данных d) Для виртуализации	ОПК-12, ОПК -13
8.	a	Какой тип сетевой атаки использует отправку Gratuitous ARP пакетов a) посредничество b) отказ в обслуживании c) распределенная атака на отказ в обслуживании d) подмена доверенного субъекта	ОПК-12, ОПК -13
9.	a	Что является самым важным при проверке безопасности новой беспроводной сети? a) Уровень шифрования b) Уровень сигнала c) Количество администраторов d) Полоса пропускания	ОПК-12, ОПК -13
10.	a	Что является объектом защиты информации? a) Компьютерная система или автоматизированная система обработки данных (АСОД) b) Вычислительные сети c) Системы управления базами данных (СУБД) d) Память ЭВМ	ОПК-12, ОПК -13
11.	a	Что является предметом защиты в компьютерных системах? a) информация b) электронные и электромеханические устройства, а также машинные носители c) системы передачи данных (СПД)	ОПК-12, ОПК -13
12.	a	Под угрозой безопасности информации понимается: a) Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности,	ОПК-12, ОПК -13

		конфиденциальности или доступности информации b) Атака на информацию со стороны злоумышленника c) Несанкционированный доступ к информации, который может привести к нарушению целостности системы компьютерной безопасности	
13.	a, b	Все множество потенциальных угроз безопасности информации в КС может быть разделено на следующие классы: a) Случайные угрозы b) Преднамеренные угрозы c) Предсказуемые угрозы d) Потенциальные угрозы	ОПК-12, ОПК -13
14.	a, b, c, d, e	Перечислите основные виды случайных угроз: a) Стихийные бедствия и аварии b) Сбои и отказы технических средств c) Ошибки при разработке компьютерных систем d) Алгоритмические и программные ошибки e) Ошибки пользователей и обслуживающего персонала f) Электромагнитные излучения и наводки g) Вредоносные программы	ОПК-12, ОПК -13
15.	a, b, c, d, e	Перечислите основные виды преднамеренных угроз: a) Шпионаж и диверсии b) Несанкционированный доступ (НСД) к информации c) Электромагнитные излучения и наводки d) Несанкционированная модификация структур e) Вредительские программы f) Алгоритмические и программные ошибки g) Стихийные бедствия и аварии	ОПК-12, ОПК -13
16.	a	Реализацию угрозы информационной безопасности называют: a) Атакой. b) Контратакой. c) Блокадой.	ОПК-12, ОПК -13

		d) Отступлением.	
17.	а	Возможность возникновения события, которое оказывает нежелательные воздействия на информацию называют: a) Угрозой. b) Ошибкой. c) Отказом. d) Сбоем.	ОПК-12, ОПК -13
18.	а	Злоумышленное действие - это действие: a) Специально направленное на нарушение конфиденциальности, целостности или доступности информации. b) Произошедшее случайным образом. c) Произошедшее под действием непреодолимых факторов.	ОПК-12, ОПК -13
19.	а	Вид атак, основанных на перегрузке и выходе из строя сетевого устройства: a) DOS. b) MSDOS. c) SOS. d) AOS.	ОПК-12, ОПК -13
20.	а	Укажите, какую функцию выполняет межсетевой экран? a) Разделение и изолирование сегментов сети b) Проверять компьютеры на наличие вирусов c) Выполнять сигнатурный анализ сетевого трафика d) Фильтрация нежелательной корреспонденции	ОПК-12, ОПК -13

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала (контрольных точек), оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

3. Критерии оценивания компетенций

Оценка «**отлично**» выставляется студенту, если он: предоставляет детальный отчёт с описанием операционных систем; критериев оценки эффективности и надежности средств защиты операционных систем; принципов организации и структуры подсистем защиты операционных систем семейства unix и windows; функций операционных систем, основных концепций управления процессорами, памятью, вспомогательной памятью, устройствами; предоставляет детальный отчёт с демонстрацией способности использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем; предоставляет детальный отчёт с демонстрацией способности применять знания в области безопасности операционных систем при разработке автоматизированных систем.

Оценка «**хорошо**» выставляется студенту в случае, когда он предоставляет отчёт с описанием операционных систем; критериев оценки эффективности и надежности средств защиты операционных систем; принципов организации и структуры подсистем защиты операционных систем семейства unix и windows; функций операционных систем, основных концепций управления процессорами, памятью, вспомогательной памятью, устройствами; предоставляет отчёт с демонстрацией способности использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем; предоставляет отчёт с демонстрацией способности применять знания в области безопасности операционных систем при разработке автоматизированных систем.

Оценка «**удовлетворительно**» выставляется студенту, если он предоставляет неполным отчёт с описанием операционных систем; критериев оценки эффективности и надежности средств защиты операционных систем; принципов организации и структуры подсистем защиты операционных систем семейства unix и windows; функций операционных систем, основных концепций управления процессорами, памятью, вспомогательной памятью, устройствами; предоставляет неполный отчёт с демонстрацией способности использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем; предоставляет неполный отчёт с демонстрацией способности применять знания в области безопасности операционных систем при разработке автоматизированных систем.

Оценка «**неудовлетворительно**» выставляется, если студент: не предоставляет отчёт с описанием операционных систем; критериев оценки эффективности и надежности средств защиты операционных систем; принципов организации и структуры подсистем защиты операционных систем семейства unix и windows; функций операционных систем, основных концепций управления процессорами, памятью, вспомогательной памятью, устройствами; не предоставляет отчёт с демонстрацией способности использовать средства операционных систем для обеспечения эффективного и безопасного

функционирования автоматизированных систем; оценивать эффективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем; не предоставляет отчёт с демонстрацией способности применять знания в области безопасности операционных систем при разработке автоматизированных систем.