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

УТВЕРЖДАЮ
Декан факультета
математики и компьютерных наук
имени профессора Н.И. Червякова
_____ Гробова Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
Защита в операционных системах

Специальность	10.05.01 «Компьютерная безопасность»
Специализация	Информационно-аналитическая и техническая экспертиза компьютерных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	5

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Защита в операционных системах». Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информацию 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 (модуля) «Защита в операционных системах»
3. Разработчик: Гусева Л.Л., доцент кафедры вычислительной математики и кибернетики.
4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель Бабенко М. Г., заведующий кафедрой вычислительной математики и кибернетики

Члены комиссии:

Тебуева Ф.Б., профессор кафедры вычислительной математики и кибернетики

Осипов Д.Л., доцент кафедры вычислительной математики и кибернетики

Представитель организации-работодателя: Березницкий А.С., главный аналитик федерального государственного бюджетного учреждения «Кабардино-Балкарская лаборатория судебной экспертизы Министерства юстиции Российской Федерации».

Экспертное заключение: Представленный ФОС по дисциплине «Защита в операционных системах» соответствует требованиям ФГОС ВО. Предлагаемые преподавателем формы и средства текущего контроля адекватны целям и задачам реализации образовательной программы высшего образования по специальности 10.05.01 Компьютерная безопасность, а также целям и задачам рабочей программы реализуемой учебной дисциплины. Оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации представлены в полном объеме.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

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

Уровни сформированности компетенци(ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ОПК-9				
Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-1 настраивает операционные системы, системы управления базами данных и компьютерные сети с учетом требований по обеспечению защиты информации	Имеет слабое представление о способах настройки операционных систем, систем управления базами данных и компьютерных сетей с учетом требований по обеспечению защиты информации	Имеет частичное представление о способах настройки операционных систем, систем управления базами данных и компьютерных сетей с учетом требований по обеспечению защиты информации	Имеет представление о способах настройки операционных систем, систем управления базами данных и компьютерных сетей с учетом требований по обеспечению защиты информации	Имеет полное представление о способах настройки операционных систем, систем управления базами данных и компьютерных сетей с учетом требований по обеспечению защиты информации
Компетенция: ОПК-12				
Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-2 выполняет резервное копирование и аварийное восстановление работоспособности прикладного и системного программного обеспечения	Имеет слабое представление о способах выполнения резервного копирования и аварийного восстановления работоспособности прикладного и системного программного обеспечения	Имеет чстичное представление о способах выполнения резервного копирования и аварийного восстановления работоспособности прикладного и системного программного обеспечения	Имеет представление о способах выполнения резервного копирования и аварийного восстановления работоспособност и прикладного и системного программного обеспечения	Имеет полное представление о способах выполнения резервного копирования и аварийного восстановления работоспособност и прикладного и системного программного обеспечения
Компетенция: ОПК-16				
Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-2 производит анализ эффективности программно-аппаратных средств защиты информации в операционных системах	Имеет слабое представление о способах производства анализа эффективности программно-аппаратных средств защиты информации в операционных системах	Имеет частичное представление о способах производства анализа эффективности программно-аппаратных средств защиты информации в операционных системах	Имеет представление о способах производства анализа эффективности программно-аппаратных средств защиты информации в операционных системах	Имеет полное представление о способах производства анализа эффективности программно-аппаратных средств защиты информации в операционных системах

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1		К какому классу безопасности относится ОС Windows по различным критериям оценки?	ОПК-9
2		Каким образом пользователи идентифицируются в ОС Windows?	ОПК-9
3		Что такое списки DACL и SACL?	ОПК-9
4		Перечислите, каким образом можно запустить процесс от имени другого пользователя.	ОПК-9
5		Как происходит проверка прав доступа пользователя к ресурсам в ОС Windows?	ОПК-9
6		Что такое маркер безопасности, и какова его роль в модели безопасности Windows?	ОПК-9
7	Cacls d:\test/рИмяКомпьютера\ИмяГруппы:f/e /t	Как с использованием команды cacls добавить права на запись для всех файлов заданной папки?	ОПК-9
8		Какие события подлежат аудиту в ОС Windows?	ОПК-9
9		Каким образом шифруются файлы в файловой системе EFS? Что такое FEK? DDF? DDR?	ОПК-12 17-4
10		Какие алгоритмы шифрования используются в EFS?	ОПК-12
11		Какова иерархия разрешений на доступ к папкам в модуле «Документы»	ОПК-12
12		Какие дополнительные атрибуты можно присвоить файлу в файловой системе ext*fs? Как эти атрибуты влияют на обеспечение конфиденциальности, целостности и доступности информации?	ОПК-12
13	Для этого можно использовать команду echo: $ echo '123' > filename	Как можно создать текстовый файл без помощи текстового редактора?	ОПК-12
14		В чем различие между копиями файла, его «жесткими» и символическими ссылками? Для чего используются символические ссылки?	ОПК-12
15		Для каких целей могут использоваться	ОПК-12

		«темные» каталоги?	
16		Какие права по отношению к файлам и каталогам вам необходимо иметь для копирования файла? Как изменяются при этом атрибуты копии?	ОПК-12
17		Администратор по невнимательности ввел следующую команду: chmod –R 555 / .Что последует за выполнением этой команды?	ОПК-12
18		Как проконтролировать действия системного сервиса syslogd?	ОПК-12
19		В каком файле необходимо установить запрет на запуск файлов со сменных машинных носителей (noexec)?	ОПК-12
20		Как просмотреть список основной и дополнительных групп пользователей?	ОПК-12
21		Какие оснастки и как можно загрузить в Active Directory	ОПК-12
22		Какую и как добавить информацию о ресурсах организации в Active Directory?	ОПК-12
23		Понятие Active Directory	ОПК-12
24		Служба Active Directory	ОПК-12
25		Компоненты Active Directory	ОПК-12
26	+: ОС, предусматривающая средства защиты от основных угроз конфиденциальности, целостности, и доступности информации.	Что называется защищенной операционной системой (ОС)? -: ОС, предусматривающая средства защиты от основных угроз конфиденциальности и целостности информации; -: ОС, предусматривающая средства защиты от основных угроз конфиденциальности и доступности информации; -: ОС, предусматривающая защиту актуальной информации; +: ОС, предусматривающая средства защиты от основных угроз конфиденциальности, целостности, и доступности информации.	ОПК-16 60-15
27	+: фрагментарный и комплексный;	Какие подходы к построению защищенных операционных систем вы знаете?	ОПК-16

		+: фрагментарный и комплексный; -: общий и частный; -: активный и пассивный; -: прикладной и комплексный.	
28	+: все вышеперечисленные.	Какие административные меры защиты вы знаете? -: постоянный контроль корректности функционирования ОС, регулярное создание резервных копий данных ОС; -: организация и поддержание адекватной политики безопасности, инструктирование пользователей ОС о необходимости соблюдений мер безопасности при работе с ОС; -: постоянный контроль изменений в конфигурационных данных и политике безопасности ОС; +: все вышеперечисленные.	ОПК-16
29	+: анализ процессов создания временных файлов ОС;	Какие этапы НЕ включает в себя формирование и поддержание адекватной политики безопасности ОС? -: анализ угроз; -: формирование требований к политике безопасности; +: анализ процессов создания временных файлов ОС; -: формальное определение политики безопасности	ОПК-16
30	+: усложнение защищенности ОС приводит к увеличению потребления ресурсов компьютера, что ведет к уменьшению объема ресурсов для прикладного ПО;	Почему неограниченный рост защищенности операционной системы (ОС) неизбежно приводит к снижению ее эксплуатационных качеств? -: усложнение защищенности ОС приводит к усложнению работы с ОС; +: усложнение защищенности ОС приводит к увеличению потребления ресурсов компьютера, что ведет к уменьшению объема ресурсов для прикладного ПО; -: усложнение защищенности ОС приводит к усложнению выполнения несанкционированных действий; -: усложнение защищенности ОС приводит к усложнению процесса загрузки ОС.	ОПК-16

31	+: все вышеперечисленное	К каким негативным последствиям может привести поддержание чрезмерно высокого уровня защищенности системы (ОС)? -: увеличение количества времени и средств, необходимых для поддержания защиты; -: отсутствие возможности нормальной работы пользователей с ОС; -: потребление значительного количества ресурсов ОС защитной системой; +: все вышеперечисленное	ОПК-16
32	+: в ситуации, когда в силу вступает новая политика безопасности;	Когда заканчивается поддержание и коррекция адекватной политики безопасности? +: в ситуации, когда в силу вступает новая политика безопасности; -: при установлении в системе нового программного продукта; -: при устранении всех угроз ОС; -: в ситуации, когда политика безопасности работает безукоризненно	ОПК-16
33	+: для исходных числовых данных, используемых в количественном анализе рисков, часто затруднительного обосновать присвоение тем или иным качественным характеристикам числовых значений;	С какими проблемами сталкиваются попытки количественного анализа рисков для тех или иных операционных систем (ОС)? +: для исходных числовых данных, используемых в количественном анализе рисков, часто затруднительного обосновать присвоение тем или иным качественным характеристикам числовых значений; -: сложность проведения количественного анализа рисков для различных систем, т.к. все системы по-своему уникальны; -: отсутствие единого перечня стандартов устранения рисков в ОС; -: сложность обоснования выбора стандартов, используемых при количественном анализе рисков ОС.	ОПК-16
34	+: стандарты безопасности могут использоваться в качестве основы для	Каковы роль и место стандартов безопасности в деле управления безопасностью операционной системы	ОПК-16

	планирования политики безопасности ОС;	(ОС)? -: стандарты безопасности являются универсальными для формирования политики безопасности ОС всех конфигураций; -: стандарты безопасности позволяют проводить количественный анализ рисков различных ОС; +: стандарты безопасности могут использоваться в качестве основы для планирования политики безопасности ОС; -: стандарты безопасности определяют конфигурацию ОС.	
35	+: возможность построить профиль защиты для ОС любой конфигурации;	Какие преимущества дает применение профилей защиты операционной системы (ОС) в стандартах безопасности компьютерных систем? +: возможность построить профиль защиты для ОС любой конфигурации; -: возможность построить профиль защиты для ОС типовых конфигураций; -: возможность отказаться от количественного анализа рисков для ОС; -: возможность отказаться от использования стандартов безопасности при построении системы безопасности ОС	ОПК-16
36	+: верны все варианты.	Какие функциональные требования из перечисленных предъявляются к безопасности операционных систем (ОС) согласно базовому профилю защиты стандарта ISO/МЭК 15408 в части, касающейся защиты данных пользователя? -: дискреционное управление доступом для заданного множества субъектов, объектов и операций над ними; -: использование уникальных идентификаторов пользователей и групп пользователей при описании политики управления доступом; -: наличие правил управления доступа, заданных по умолчанию и применяемых, когда атрибуты	ОПК-16

		безопасности субъекта не соответствуют атрибутам безопасности объекта; +: верны все варианты.	
37	+: использование уникальных идентификаторов пользователей и групп пользователей при описании политики управления доступом;	Какие функциональные требования из перечисленных НЕ предъявляются к безопасности операционных систем согласно базовому профилю защиты стандарта ISO/МЭК 15408 в части, касающейся идентификации и аутентификации? -: ограничение максимально возможного количества неуспешных попыток аутентификации в одном подключении к операционной системе; +: использование уникальных идентификаторов пользователей и групп пользователей при описании политики управления доступом; -: требования к стойкости механизмов верификации секретов к подбору аутентификационной информации; -: явное ограничение списка действий, возможных для неидентифицированного или неаутентифицированного пользователя.	ОПК-16
38	+: наличие механизма квотирования оперативной памяти, процессорного времени и, возможно, других аппаратных ресурсов;	Какие функциональные требования из перечисленных НЕ предъявляются к безопасности операционных систем согласно базовому профилю защиты стандарта ISO/МЭК 15408 в части, касающейся защиты функций безопасности? +: наличие механизма квотирования оперативной памяти, процессорного времени и, возможно, других аппаратных ресурсов; -: возможность самотестирования подсистемы безопасности операционной системы при запуске, периодически во время работы или по запросу уполномоченного администратора; -: обеспечение конфиденциальности и целостности внутренних данных подсистем безопасности операционных систем в процессе их	ОПК-16

		сетевого взаимодействия; -: наличие средств восстановления подсистемы безопасности операционной системы после сбоев и аварий	
39	+: все вышеперечисленные.	Какие функциональные требования из перечисленных предъявляются к безопасности операционных систем согласно базовому профилю защиты стандарта ISO/МЭК 15408 в части, касающейся доступа к операционной системе?	ОПК-16
40	+: любой элемент операционной системы, доступ к которому пользователей и других субъектов доступа может быть произвольно ограничен;	Что называется объектом доступа?	ОПК-16
41	+: любая сущность, способная инициировать выполнение операций над объектами	Что называется субъектом доступа?	ОПК-16
42	+: операция, определенная для некоторого объекта;	Что называется методом доступа?	ОПК-16
43		Иерархия доменов	ОПК-16
44		Учетные записи пользователей	ОПК-16
45		Доверительные отношения	ОПК-16
		Групповые политики	ОПК-16
46		Структура каталога Active Directory	ОПК-16
47		Active Directory и LDAP	ОПК-16
48		Физическая структуризация	ОПК-16
49		Как добавить глобальную группу в оснастку Active Directory?	ОПК-16
50		Как добавить комментарий в объект групповой политики?	ОПК-16
51		Как настроить параметр «Таймаут экранной заставки»?	ОПК-16
52		Как посмотреть отчет о параметрах в объекте GPO?	ОПК-16
53		Как изменить политику «Всегда ждать	ОПК-16

		сеть при запуске и входе в систему»	
54		1. Как добавить группу с ограниченным доступом?	ОПК-16
55		Как группе присвоить права администратора?	ОПК-16
56		Как связать несколько объектов GPO?	ОПК-16
57		Как разрешить вход на удаленный рабочий стол?	ОПК-16
58		Как создать шаблон удаленного рабочего стола?	ОПК-16
60		Что называется правом доступа субъекта к объекту?	ОПК-16

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».

Рейтинговая система оценки не предусмотрено для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной формы обучения.

3. Критерии оценивания компетенций

Оценка «отлично» выставляется, если студент:

- имеет полное представление о способах настройки операционных систем, систем управления базами данных и компьютерных сетей с учетом требований по обеспечению защиты информации.

Оценка «хорошо» выставляется, если студент:

- имеет представление о способах настройки операционных систем, систем управления базами данных и компьютерных сетей с учетом требований по обеспечению защиты информации.

Оценка «удовлетворительно» выставляется, если студент:

- имеет частичное представление о способах настройки операционных систем, систем управления базами данных и компьютерных сетей с учетом требований по обеспечению защиты информации.

Оценка «неудовлетворительно» выставляется, если студент:

- имеет слабое представление о способах настройки операционных систем, систем управления базами данных и компьютерных сетей с учетом требований по обеспечению защиты информации.