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
Модели безопасности компьютерных систем

Специальность	10.05.01 Компьютерная безопасность
Специализация	Информационно-аналитическая и техническая экспертиза компьютерных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	8

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Модели безопасности компьютерных 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 (модуля) «Модели безопасности компьютерных систем»

3. Разработчик: Свистунов Николай Юрьевич, ассистент 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
Гусева Л.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 «Модели безопасности компьютерных систем» 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 компетенции(ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (неудовлетвори-тельно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ОПК-8				
Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-1$_{ОПК-8}$ ИД-2$_{ОПК-8}$	Не способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	Способен на базовом уровне применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	Способен на хорошем уровне применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей. Владеет на углубленном уровне методологией научных исследований при проведении разработок в области защиты информации
Компетенция: ОПК-11				
Индикатор: ИД-2$_{ОПК-11}$	Не способен разрабатывать политики безопасности, политики управления доступом и информационным и потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	Способен на базовом уровне разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	Способен на хорошем уровне разрабатывать политики безопасности, политики управления доступом и информационным и потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	В полной мере способен разрабатывать политики безопасности, политики управления доступом и информационным и потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации

Оценочные средства для проверки уровня сформированности компетенций
8 семестр

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1	б) монитор безопасности объектов	Монитор обращений, который разрешает поток, принадлежащий только множеству легального доступа а) монитор доступа к данным б) монитор безопасности объектов в) монитор безопасности субъектов г) монитор порождения субъектов	ОПК-8
2	б) модели Белла-ЛаПадулы	Использование аксиом «не читать ниже» и «не записывать выше» характерно для а) модели АДЕПТ-50 б) модели Белла-ЛаПадулы в) пространства безопасности Хартстона г) модели low-water-mark	ОПК-8
3	а) дискреционное	… разграничение доступа реализуется обычно в виде матрицы доступа, строки которой соответствуют субъектам компьютерной системы, а столбцы – ее объектам. а) дискреционное б) ролевое в) мандатное	ОПК-8
4	а) паравиртуализация	Техника виртуализации, при которой гостевые операционные системы подготавливаются для исполнения в виртуализированной среде а) паравиртуализация б) эмуляция в) аппаратная виртуализация г) виртуализация приложений	ОПК-8
5	в) уровень безопасности	При полномочной политике безопасности совокупность меток с одинаковыми значениями образует а) область равной критичности б) область равного доступа в) уровень безопасности г) уровень доступности	ОПК-8
6	в) сложность реализации	Недостатком модели конечных состояний политики безопасности является а) изменение линий связи б) статичность в) сложность реализации г) низкая степень надежности	ОПК-8
7	б) относительно низкая производительность	Недостаток систем шифрования с открытым ключом а) при использовании простой замены легко произвести подмену одного шифрованного текста другим б) относительно низкая производительность в) необходимость распространения секретных ключей г) на одном и том же ключе одинаковые блоки открытого текста перейдут в одинаковые блоки шифрованного текста	ОПК-8
8	а) изначальное допущение вскрываемости системы	Недостатком модели политики безопасности на основе анализа угроз системе является	ОПК-8

		а) изначальное допущение вскрываемости системы б) статичность в) необходимость дополнительного обучения персонала г) сложный механизм реализации	
9	б) пользователями	Полномочия подсистем ядра безопасности ОС ассоциируются с а) процессами б) пользователями в) периферийными устройствами г) приложениями	ОПК-8
10	г) авторизация	Предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы – это а) идентификация б) аудит в) аутентификация г) авторизация	ОПК-8
11	а) процесс winlogon	Регистрацией в системе Windows управляет а) процесс winlogon б) процесс lsass в) библиотека msgina.dll г) библиотека logon.dll	ОПК-8
12	в) сеансовом	Поддержка диалога между удаленными процессами реализуется на … уровне модели взаимодействия открытых систем а) сетевом б) транспортном в) сеансовом г) канальном	ОПК-8
13	Достоверность Свойство достоверности	___ – сохранение информацией своих свойств в любой момент времени, начиная с её ввода в систему	ОПК-8
14	Доступность Свойство доступности	___ – возможность пользования некоторым ресурсом КС и информацией в произвольный момент времени	ОПК-8
15	Целостность Свойство целостности	___ – неизменность свойств информации и ресурсов в любой момент времени	ОПК-8
16	Конфиденциальность Свойство конфиденциальности	___ – недоступность информации или сервисных услуг КС для лиц, которые не имеют на это соответствующего разрешения или допуска, санкционированного руководством организации	ОПК-8
17	причины	Несоответствие (неадекватность) политики безопасности реальным условиям жизненного цикла КС, ошибки управления системой безопасности, ошибки проектирования системы гарантий, ошибки программной реализации – это ___ реализации угроз	ОПК-8
18	create	Операция ___ задает отображение декартова произведения множеств субъектов и объектов на объединение множества субъектов с пустым множеством	ОПК-8
19	stream	Операция ___ может создавать новый объект или уничтожать его	ОПК-8
20	изолированным	Множество субъектов КС называется ___	ОПК-8

		если в ней действует монитор безопасности субъектов и субъекты из порождаемого множества корректны относительно друг друга и монитора безопасности субъектов	
21	индикаторный	___ монитор обращений устанавливает только факт обращения субъекта к объекту, но не оказывает влияния на порождаемые потоки данных	ОПК-8
22		С применением каких основных понятий построены классические модели и ДП-модели безопасности?	ОПК-8
23		Сформулируйте основную аксиому компьютерной безопасности	ОПК-8
24		В чём состоит сущность модели Харрисона-Руззо-Ульмана?	ОПК-8
25		В каком случае начальное состояние системы ХРУ называется безопасным относительно некоторого права доступа?	ОПК-11
26		Возможна ли алгоритмическая проверка безопасности произвольных систем ХРУ?	ОПК-11
27		Что такое система монотонной типизированной матрицы доступа (МТМД)?	ОПК-11
28		Какую структуру называют мостом в графе доступов?	ОПК-11
29		В каком случае Объект *o* в момент времени *t* функционально ассоциирован с субъектом *s*?	ОПК-11
30		Что такое монитор обращений?	ОПК-11
31		Что такое монитор безопасности объектов?	ОПК-11
32		В каком случае два субъекта компьютерной системы являются корректными относительно друг друга?	ОПК-11
33		Что такое монитор порождения субъектов?	ОПК-11
34		Что такое монитор безопасности субъектов?	ОПК-11
35		При соблюдении какого условия компьютерная система называется замкнутой по порождению субъектов?	ОПК-11
36		В каком случае программная среда называется изолированной?	ОПК-11
37		Сформулируйте базовую теорему изолированной программной среды	ОПК-11
38		Какие особенности функционирования современных компьютерных систем не учитываются в классических моделях безопасности?	ОПК-11
39		Дайте определение функционально корректного доверенного субъекта.	ОПК-11
40		Обеспечение безопасности состояний и функции переходов в контексте модели Белла-ЛаПадулы недостаточно для противодействия возможности реализации каких видов запрещённых информационных потоков?	ОПК-11
41		Что понимается под нарушением безопасности веб-системы?	ОПК-11
42		Опишите типовой жизненный цикл защищённой компьютерной системы.	ОПК-11

43		Какие действия программного субъекта приводят к его определению как некорректного?	ОПК-11
44		Что такое контекст вызова программного субъекта?	ОПК-11
45		Какие методы анализа программного обеспечения относятся к динамическим?	ОПК-11
46		Дайте определение защищённого хранилища пользователя.	ОПК-11
47		Что понимается под публичным представлением пользователя?	ОПК-11
48		Дайте определение способа доступа к содержимому контейнера в контексте модели систем военных сообщений.	ОПК-11
49		Что понимается под сообщением в контексте модели систем военных сообщений?	ОПК-11
50		Какие основные операции над сущностями имеются в модели систем военных сообщений?	ОПК-11
51		Назовите постулаты безопасности системы военных сообщений.	ОПК-11

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 студенту, если он способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей; владеет на углубленном уровне методологией научных исследований при проведении разработок в области защиты информации; в полной мере способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.

Оценка «хорошо» выставляется студенту, если он способен на хорошем уровне применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей; способен на хорошем уровне разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.

Оценка «удовлетворительно» выставляется студенту, если он способен на базовом уровне применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей; способен на базовом уровне разрабатывать политики безопасности, политики управления доступом и

информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;

Оценка «неудовлетворительно» выставляется студенту, если он в недостаточной степени способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей; не способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.