Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гробова Татьяна Анатольевна
Должность: и.о. декана факультета математики и компьютерных наук имени профессора Н.И. Червякова
Дата подписания: 19.06.2026 15:22:57
Уникальный программный ключ:
bd39d4208aa94cf4422feb787c816191d2da70a7

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

Методы и стандарты оценки защищенности информационных систем

Направление подготовки	10.04.01 Информационная безопасность
Направленность (профиль)	Математическое и программное обеспечение защиты информации
Форма обучения	очная
Год начала обучения	2026
Реализуется в 1 семестре	

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Методы и стандарты оценки защищенности информационных систем». 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) «Методы и стандарты оценки защищенности информационных систем»

3. Разработчик: Рябцев С.С.., старший преподаватель кафедры вычислительной математики и кибернетики

4. Проведена экспертиза ФОС.

Члены экспертной группы:

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

Члены комиссии: Осипов Д.Л., доцент кафедры вычислительной математики и кибернетики

Гусева Л.Л., доцент кафедры вычислительной математики и кибернетики

Представитель организации-работодателя: Березницкий А.С., кандидат экономических наук, главный аналитик ФБУ «Северо-Кавказского регионального центра судебной экспертизы Министерства юстиции РФ» ФГБУ Кабардино-Балкарской лаборатории судебной экспертизы Министерства юстиции Российской Федерации.

Экспертное заключение: Представленный ФОС по дисциплине «Методы и стандарты оценки защищенности информационных систем» соответствует требованиям ФГОС ВО. Предлагаемые преподавателем формы и средства текущего контроля адекватны целям и задачам реализации образовательной программы высшего образования по направлению 10.04.01 Информационная безопасность направленность (профиль) «Математическое и программное обеспечение защиты информации», 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
ИД-1 ПК-1 разрабатывает требования по защите информации компьютерной системы	Допускает грубые ошибки при разработке требования по защите информации в компьютерных сетях с учетом требований стандартов безопасности.	частично разрабатывает требования по защите информации в компьютерных сетях с учетом требований стандартов безопасности.	Разрабатывает требования по защите информации в компьютерных сетях с учетом требований стандартов безопасности.	Самостоятельно и творчески разрабатывает требования по защите информации в компьютерных сетях с учетом требований стандартов безопасности.
ИД-2 ПК-1 разрабатывает профили защиты компьютерных систем и формулирует задания по безопасности компьютерных систем	Допускает грубые ошибки при осуществлении управления информационной безопасности.	С помощью преподавателя осуществляет поиск, сбор и частично обработку информации для определения альтернативных вариантов стратегических действий в проблемной ситуации	Осуществляет поиск, сбор и обработку информации для определения альтернативных вариантов стратегических действий в проблемной ситуации	Самостоятельно и творчески осуществляет детальный поиск, сбор и обработку информации для определения альтернативных вариантов стратегических действий в проблемной ситуации
ИД-3 ПК-1 формирует политики безопасности компьютерных систем и сетей	Допускает грубые ошибки при разработке и документации политики сетевой безопасности.	С помощью преподавателя разрабатывает и документирует политики сетевой безопасности.	Разрабатывает и документирует политики сетевой безопасности.	Самостоятельно и творчески разрабатывает и документирует политики сетевой безопасности.
ИД-1 ПК-2 оценивает работоспособность применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик	Допускает грубые ошибки при анализе защищенности компьютерных систем с использованием сканеров безопасности.	Предоставляет частичный отчет об анализе защищенности компьютерных систем с использованием сканеров безопасности.	Выполняет анализ защищенности компьютерных систем с использованием сканеров безопасности.	Предоставляет детальный отчет о анализе защищенности компьютерных систем с использованием сканеров безопасности
ИД-2 ПК-2 оценивает эффективность применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик	Допускает грубые ошибки в применении методов анализа защищенности компьютерных систем и сетей.	Частично применяет методы анализа защищенности компьютерных систем и сетей.	Применяет методы анализа защищенности компьютерных систем и сетей.	Самостоятельно и творчески применяет методы анализа защищенности компьютерных систем и сетей.
ИД-1 ПК-3 выполняет анализ	Допускает грубые ошибки в применении	Частично применяет	Применяет инструментальны	Самостоятельно и творчески

защищенности компьютерных систем с использованием сканеров безопасности	инструментальных средства проведения мониторинга защищенности компьютерных систем.	инструментальные средства проведения мониторинга защищенности компьютерных систем.	е средства проведения мониторинга защищенности компьютерных систем.	применяет инструментальные средства проведения мониторинга защищенности компьютерных систем.
ИД-2 ПК-3 выполняет анализ защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей	Допускает грубые ошибки при анализе защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составления отчетов по результатам проверок.	С помощью преподавателя выполняет анализ защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составления отчетов по результатам проверок.	Выполняет анализ защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составления отчетов по результатам проверок.	Самостоятельно и творчески выполняет анализ защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составления отчетов по результатам проверок.

Оценочные средства для проверки уровня сформированности компетенций
4 семестр

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1.		Модели пересчёта справочных показателей долговечности элементов с учётом электрического режима и температуры.	ПК-1
2.		Принцип определения показателей долговечности и показателей сохраняемости ЭУ.	ПК-1
3.		Оценка надёжности технической системы методом прямого перебора работоспособных состояний.	ПК-1
4.	+: это наносящие ущерб владельцу коммерческой тайны, незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не	Что такое промышленный шпионаж: +: это наносящие ущерб владельцу коммерческой тайны, незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем. -: это наносящие ущерб пользователю не коммерческой тайны, незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем. -: это наносящие ущерб владельцу не коммерческой тайны, законный сбор, присвоение и передача сведений, составляющих не коммерческую тайну, лицом, не уполномоченным на это ее владельцем -: это наносящие ущерб пользователю не коммерческой тайны, незаконный сбор,	ПК-1

		присвоение и передача сведений, составляющих коммерческую тайну, лицом, уполномоченным на это ее владельцем	
5.	+: разглашения конфиденциальной информации +: несанкционированного доступа к конфиденциальной информации различными способами	Следствия утечки конфиденциальной информации: +: разглашения конфиденциальной информации +: несанкционированного доступа к конфиденциальной информации различными способами -: разглашение публичной информации -: санкционированного доступа к конфиденциальной информации различными способами	ПК-1
6.	+: это стирание ее в памяти ЭВМ, удаление с физических носителей, а также несанкционированные изменения составляющих ее данных, кардинально меняющие содержание.	Что такое уничтожение компьютерной информации ? +: это стирание ее в памяти ЭВМ, удаление с физических носителей, а также несанкционированные изменения составляющих ее данных, кардинально меняющие содержание. -: это удаление файлов с рабочего стола -: это стирание ее в памяти ЭВМ, а также с внешнего носителя -: это удаление файлов ее в памяти ЭВМ, удаление с физических носителей, а также санкционированные изменения составляющих ее данных, кардинально меняющие содержание.	ПК-2
7.	+: это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением.	Что такое блокирование компьютерной информации ? -: это искусственное затруднение доступа одного пользователя к компьютерной информации, и связанное с ее удалением. -: это искусственное затруднение доступа пользователей к компьютерной информации, и связанное с ее уничтожением. +: это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением. -: это затруднение владельца к своей компьютерной информации	ПК-2
8.	+: программа, выполняющая в дополнение к основным (проектным и документированным) не описанные в	Троянский конь – это : +: программа, выполняющая в дополнение к основным (проектным и документированным) не описанные в документации действия. -: программа для удаления вирусов	ПК-2

	документации действия.	-: полезная утилита для ЭВМ -: программа для редактирования файлов.	
9.	+: программа, которая может заражать другие программы путем включения в них своей, возможно модифицированной, копии, причем последняя сохраняет способность к дальнейшему размножению.	Вирус – это ? -: программа для общения пользователей +: программа, которая может заражать другие программы путем включения в них своей, возможно модифицированной, копии, причем последняя сохраняет способность к дальнейшему размножению. -: утилита для безопасного доступа к облачному хранению. -: сайт для удаленного доступа.	ПК-2
10.	+: программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе.	Что такое червь ? -: программа, распространяющаяся через твердотельный накопитель. -: утилита для редактирования фотографий. -: программа, распространяющаяся через сеть и оставляющая свою копию на магнитном носителе. +: программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе.	ПК-2
11.	+: пути передачи информации между процессами системы, нарушающие системную политику безопасности.	Что такое скрытые каналы ? +: пути передачи информации между процессами системы, нарушающие системную политику безопасности. -: пути передачи информации между процессами системы, не нарушающие системную политику безопасности. -: пути передачи скрытой информации -: путь для передачи взломанного ПО	ПК-2
12.	+: умышленное проникновение в систему с несанкционированными параметрами входа, то есть именем пользователя и его паролем.	Взлом системы это ? -: установка старых драйверов системы -: установка не лицензированного ПО -: умышленное проникновение в систему с санкционированными параметрами входа, то есть именем пользователя и его паролем. +: умышленное проникновение в систему с несанкционированными параметрами входа, то есть именем пользователя и его паролем.	ПК-3
13.	+: Люком называется не описанная в документации на программный продукт	Дайте определение понятию «Люки» : -: Люком называется описанная в документации на программный язык	ПК-3

	возможность работы с этим программным продуктом.	продукт и не возможность работы с этим программным продуктом. -: Люком называется описанная в документации на программный продукт возможность работы с этим программным продуктом. +: Люком называется не описанная в документации на программный продукт возможность работы с этим программным продуктом. -: Люком называется доступ к программе путем подхвата вируса.	
14.	+: сложность сбора доказательств и процесса доказывания в суде -: использование программных "ловушек" +: отсутствие достаточной следственной практики по расследованию компьютерных преступлений в Российской Федерации	Какие особенности характерны для компьютерных преступлений? -: копирование машинных носителей информации +: сложность сбора доказательств и процесса доказывания в суде -: использование программных "ловушек" +: отсутствие достаточной следственной практики по расследованию компьютерных преступлений в Российской Федерации	ПК-3

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 студент показал глубокое, прочное и аргументированное знание программного учебного материала дисциплины, при этом поставленные вопросы раскрывает последовательно, четко и логически стройно, в полном исчерпывающем объеме; умеет правильно формулировать, и владеет основными категориями, понятиями и терминами по материалам дисциплины, не допускает при ответе ошибок, владеет инновационными приемами работы. Если он проявил самостоятельность, организованность, добросовестность творческий подход при подготовке доклада, выраженное стремление к приобретению и совершенствованию профессиональных знаний, умений и навыков.

Оценка «хорошо» выставляется студенту в случае, когда студент в основном знает программный учебный материал дисциплины, поставленные в докладе вопросы раскрывает последовательно, четко и логически стройно, но допускает незначительные неточности. Умеет правильно формулировать, и владеет основными категориями, понятиями и терминами по материалам доклада, однако допускает при ответе отдельные неточности или одну, две ошибки; не отличался инициативностью, высокой активностью, творческим подходом и самостоятельностью в выполнении доклада. В основном владеет инновационными приемами работы.

Оценка «удовлетворительно» выставляется студенту за: наличие поверхностных знаний, неустойчивых умений в области профессиональной деятельности; дает не полные ответы на поставленные в докладе вопросы, показал слабое владение инновационными приемами работы; отсутствие должностной инициативности, самостоятельности и творчества при подготовке доклада.

Оценка «неудовлетворительно» выставляется, если студент допускает грубые ошибки при ответе на вопросы по докладу, знает на недостаточно высоком уровне материал доклада и не в полной мере готов по подготовленному докладу.