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 «Информационная безопасность распределенных центров обработки данных»

Специальность	Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная

Реализуется в 9 семестре

Введение

1. Назначение: Фонд оценочных средств предназначен для обеспечения методической основы для организации и проведения текущего контроля по дисциплине «Информационная безопасность распределенных центров обработки данных». 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 «Информационная безопасность распределенных центров обработки данных»

3. Разработчик: Беликов А.О., 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:

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: ПК-1.				
Результаты обучения по дисциплине (модулю): Индикатор: ИД-1ПК- Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.	Не предоставляет отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.	Предоставляет неполный отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.	Предоставляет отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.	Предоставляет детальный отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.
ИД-2ПК-1 Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей.	Не предоставляет отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей.	Предоставляет неполный отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей.	Предоставляет отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей.	Предоставляет детальный отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей.
ИД-3ПК-1. Проведение анализа безопасности компьютерных систем.	Не предоставляет отчёт по результатам проведения анализа безопасности	Предоставляет неполный отчёт по результатам проведения анализа безопасности компьютерных систем.	Предоставляет отчёт по результатам проведения анализа безопасности компьютерных систем.	Предоставляет детальный отчёт по результатам проведения анализа безопасности компьютерных систем.

ИД-4ПК-1 Проведение сертификации программно-аппаратных средств защиты информации и анализ результатов.	Не предоставляет отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.	Предоставляет неполный отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.	Предоставляет отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.	Предоставляет детальный отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.
ИД-5ПК-1 Проведение инструментального мониторинга защищенности компьютерных систем и сетей.	Не предоставляет отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей.	Предоставляет неполный отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей.	Предоставляет отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей.	Предоставляет детальный отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей.
ИД-6ПК-1 Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.	Не предоставляет отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.	Предоставляет неполный отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.	Предоставляет отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.	Предоставляет детальный отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений 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
		Форма обучения очная/заочная/очно-заочная	
1.	Правовые, организационные и технические основы защиты сведений, составляющих государственную тайну, а также иной конфиденциальной информации от несанкционированного доступа, перехвата и утечки с использованием технических средств разведки.	Положение о государственной системе защите информации в Российской Федерации от иностранных технических разведок и от её утечки по техническим каналам определяет:	ПК-1
2.	нормативными правовыми актами, устанавливающими порядок организации и осуществления защиты государственной тайны и конфиденциальной информации от иностранного технического	«Положение о государственной системе защите информации в Российской Федерации от иностранных технических разведок и от её утечки по техническим каналам» и «Инструкция по обеспечению режима секретности в Российской Федерации определяет» являются:	ПК-1

	шпионажа и несанкционированного доступа в Российской Федерации.		
3.	порядок организации и соблюдения режима секретности при работе с государственной тайной, включая правила доступа, учёта, хранения, передачи и уничтожения носителей секретной информации, а также меры ответственности за нарушения.	«Инструкция по обеспечению режима секретности в Российской Федерации» определяет:	ПК-1
4.	a, b, c	Главными направлениями работ по ЗИ являются: a) обеспечение эффективности управления СЗИ b) разработка организационно-технических мероприятий по ЗИ и их реализация c) организация и проведение контроля состояния ЗИ d) сохранение возможности управления процессом обработки и пользования информацией e) организация лицензирования деятельности организаций организация и проведение специальных экспертиз	ПК-1
5.	a	Организация работ по защите информации на предприятиях осуществляется: a) их руководителями	ПК-1

		b) специалистами по защите информации c)) штатными сотрудниками отдела по защите информации	
6.	a	Для проведения работ по защите информации могут привлекаться специализированные предприятия, имеющие ### на право проведения работ в области защиты информации. a) лицензию b) аттестат c) сертификат	ПК-1
7.	a, c	Целями защиты являются: a) предотвращение утечки информации по техническим каналам b) предотвращения перехвата техническими средствами информации, передаваемой по каналам связи c) соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах обработки d) предотвращения специальных программно- технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств автоматизации	ПК-1
8.	b, d	Защита информации осуществляется путем a) предотвращение утечки информации по техническим каналам b) предотвращения перехвата техническими средствами информации, передаваемой по каналам связи c) соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах обработки d) предотвращения специальных программно- технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств автоматизации	ПК-1
9.	a	Предотвращение перехвата техническими средствами информации, предаваемой по линиям связи, достигается применением ### и иных методов и средств защиты, а также проведением организационно-технических и режимных мероприятий a) криптографических b) технических	ПК-1

		c) аппаратных	
10.	a	Какие вирусы активизируются в самом начале работы с операционной системой: a) загрузочные вирусы b) троянцы c) черви	ПК-1
11.	c	По «среде обитания» вирусы можно разделить на: a) не опасные b) очень опасные c) файловые	ПК-1
12.	c	Какие угрозы безопасности данных являются преднамеренными: a) ошибки персонала b) открытие электронного письма, содержащего вирус c) не авторизованный доступ	ПК-1
13.	c	По «среде обитания» вирусы можно разделить на: a) Опасные b) не опасные c) макровирусы	ПК-1
14.	c	Под какие системы распространение вирусов происходит наиболее динамично: a) Windows b) Mac OS c) Android	ПК-1
15.	a	Макровирусы: a) существуют для интегрированного офисного приложения Microsoft Office b) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске заражают загрузочный сектор гибкого или жёсткого диска	ПК-1
16.	b	Какой вид идентификации и аутентификации получил наибольшее распространение: a) системы PKI b) постоянные пароли c) одноразовые пароли	ПК-1
17.		Файловые вирусы: a) заражают загрузочный сектор гибкого или жёсткого диска	

	c	b) существуют для интегрированного офисного приложения Microsoft Office c) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске	ПК-1
18.	b	Для периодической проверки компьютера на наличие вирусов используется: a) Компиляция b) антивирусное сканирование c) дефрагментация диска	ПК-1
19.	c	Антивирусный сканер запускается: a) автоматически при старте операционной системы и работает в качестве фонового системного процессора, проверяя на вредоносность совершаемые другими программами действия b) оба варианта верны c)) по заранее выбранному расписанию или в произвольный момент пользователем. Производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера	ПК-1
20.	c	Какие состояния защищенности информации являются основой безопасной IT-инфраструктуры? a) Конфиденциальность, доступность, подлинность b) Конфиденциальность, целостность, подлинность c) Конфиденциальность, целостность, доступность d) Целостность, доступность, подлинность	ПК-1
21.	d	Какие существуют степени секретности сведений, составляющих государственную тайну? a) Особой важности, абсолютно секретно, совершенно секретно b) Абсолютно секретно, совершенно секретно, секретно c) Особой важности, абсолютно секретно, секретно d) Особой важности, совершенно секретно, секретно	ПК-1
22.	c	Какие сведения НЕ относятся к конфиденциальной информации? a) Персональные данные b) Коммерческая тайна c) Сведения об имуществе организации d) Данные о ведении расследования и судебные документы	ПК-1
23.		Что из перечисленного НЕ относится к объектам защиты конфиденциальной	

	d	информации? a) Информация b) Ресурсные объекты c) Физические объекты d) Социальные объекты	ПК-1
24.	d	Какое свойство информации понимается под «состоянием ресурсов автоматизированной информационной системы, при котором обеспечивается реализация информационной технологии с использованием именно тех ресурсов, к которым субъект, имеющий на это право, обращается». a) Целостность b) Доступность c) Подотчетность d) Подлинность	ПК-1
25.	a	Какой термин понимается под «совокупностью условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации» a) Угроза b) Уязвимость c) Утечка d) Перехват	ПК-1
26.	d	Какие сведения НЕ относятся к государственной тайне? a) Сведения в военной области b) Сведения в области экономики, науки и техники c) Сведения в области внешней политики и экономики d) Сведения о государственных валютных резервах	ПК-1
27.	b	Какому принципу с позиции системного подхода НЕ обязана удовлетворять система защиты информации? a) Непрерывность b) Совершенность c) Целенаправленность и конкретность d) Надежность, универсальность и комплексность	ПК-1
28.		Что из перечисленного НЕ относится к основным задачам технической защиты информации?	

	d	a) Предотвращение утечки информации через технические каналы b) Предотвращение несанкционированного доступа к информации c) Защита носителей информации от уничтожения d) Защита от несанкционированного использования программ	ПК-1
29.	c	Что из перечисленного НЕ относится к защищаемым объектам информатизации? a) Средства и системы информатизации b) Технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается c) Технические средства и системы, не обрабатывающие конфиденциальную информацию d) Защищаемые помещения	ПК-1

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала, оптимально расположенных на всем временном интервале изучения дисциплины.

3. Критерии оценивания компетенций*

Оценка «**зачтено**» выставляется студенту, если студент знает ключевых понятия, демонстрирует понимание основных терминов, принципов и теоретических основ дисциплины, материал излагается логично, с выделением причинно-следственных связей и примеров, используются рекомендованные учебные материалы, а также дополнительные достоверные источники, работы (индивидуальные, групповые, проектные) сданы в установленные сроки и соответствуют требованиям, студент корректно использует изученные методики, инструменты или технологии, в работах присутствуют обоснованные заключения, а в случае проектов – практическая значимость.

Оценка «**не зачтено**» выставляется студенту в следующих случаях: неудовлетворительное освоение программы: не продемонстрировано понимание базовых понятий и принципов дисциплины в работах содержатся грубые теоретические ошибки отсутствует логика в изложении материала ответы не соответствуют поставленным вопросам, невыполнение практических требований: работа не сдана в установленный срок без уважительной причины практические задания выполнены менее чем на 50% от требуемого объема нарушены методические требования к оформлению работ обнаружен плагиат (более 50% заимствованного текста без указания источников).