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

Компьютерные вирусы и борьба с ними

Специальность	10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль)	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	7

Предисловие

1. Назначение: проведение текущего контроля успеваемости и промежуточной аттестации по дисциплине «Математические методы теории сигналов».

2. ФОС является приложением к программе дисциплины «Математические методы теории сигналов».

3. Разработчики: Пелешенко Виктор Сергеевич, 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:
Лапина М. А. – доцент кафедры вычислительной математики и кибернетики
Пелешенко Т. А. – доцент кафедры вычислительной математики и кибернетики

Представитель организации-работодателя:
Корниенко С. А. — Представитель организации-работодателя начальник управления филиала ФГУП «Главный радиочастотный центр» в Южном и Северо-Кавказском федеральных округах»

Экспертное заключение: фонд оценочных средств рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Математические методы теории сигналов».
«___»_____2026 г.

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. Способен оценивать уровень безопасности компьютерных систем и сетей**				
Результаты обучения по дисциплине: *Индикатор:* **ИД-1$_{ПК-1}$** Проводит контрольные проверки 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.
Результаты обучения по дисциплине: *Индикатор:* **ИД-2$_{ПК-1}$** Разрабатывает требования 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.
Результаты	Не	Предоставляе	Предоставляет	Предоставляет

обучения по дисциплине: *Индикатор:* **ИД-3$_{ПК-1}$** Проводит анализ безопасности компьютерных систем.	предоставляет отчёт по результатам проведения анализа безопасности компьютерных систем.	т неполный отчёт по результатам проведения анализа безопасности компьютерных систем.	отчёт по результатам проведения анализа безопасности компьютерных систем.	детальный отчёт по результатам проведения анализа безопасности компьютерных систем.
Результаты обучения по дисциплине: *Индикатор:* **ИД-4$_{ПК-1}$** Проводит сертификацию 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 по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.	Предоставляет по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.
Результаты обучения по дисциплине: *Индикатор:* **ИД-5$_{ПК-1}$** Проводит инструментальный мониторинг 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.
Результаты обучения по дисциплине: *Индикатор:* **ИД-6$_{ПК-1}$** Проводит экспертизу при расследовании	Не предоставляет отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушени	Предоставляет неполный отчёт по результатам проведения экспертизы при расследовани и компьютерны	Предоставляет отчет по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушен	Предоставляет детальный отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушени й и инцидентов.

компьютерных преступлений, правонарушений и инцидентов.	й и инцидентов.	х преступлений, правонарушений и инцидентов.	ий 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
1.	a	Утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами: a) Руткит b) Бэкап c) Камбэк	ПК-1
2.	b	Компьютерные вирусы: a) файлы, которые невозможно удалить b) программы, способные к саморазмножению(самокопированию) c) файлы, имеющие определенное расширение	ПК-1
3.	c	DDos — программы: a) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера b) оба варианта верны c) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров	ПК-1
4.	a	Отличительными способностями компьютерного вируса являются: a) способность к самостоятельному запуску и многократному копированию кода + b) значительный объем программного кода c) легкость распознавания	ПК-1
5.	c	DoS — программы:	ПК-1

		a) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров b) оба варианта верны c) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера	
6.	b	Компьютерные вирусы: a) являются следствием ошибок в операционной системе b) пишутся людьми специально для нанесения ущерба пользователем ПК возникают в связи со сбоями в аппаратных средствах компьютера	ПК-1
7.	c	Троянские программы бывают: a) сетевые программы b) программы передачи данных программы — шпионы	ПК-1
8.	a	Основная масса угроз информационной безопасности приходится на: a) Троянские программы b) Шпионские программы c) Черви	ПК-1
10.	a	Информационная безопасность зависит от: a) компьютеров, поддерживающей инфраструктуры b) пользователей c) информации	ПК-1
11.	a	Сетевые черви бывают: a) Web-черви b) черви операционной системы	ПК-1

		c) черви MS Office	
12.	b	Таргетированная атака – это: a) атака на сетевое оборудование b) атака на компьютерную систему крупного предприятия c) атака на конкретный компьютер пользователя	ПК-1
13.	a	Сетевые черви бывают: a) почтовые черви b) черви операционной системы c) черви MS Office	ПК-1
14.	c	Stuxnet – это: a) троянская программа b) макровирус c) промышленный вирус	ПК-1
15.	a	По «среде обитания» вирусы можно разделить на: a) загрузочные b) очень опасные c) опасные	ПК-1
16.	a	Какие вирусы активизируются в самом начале работы с операционной системой: a) загрузочные вирусы b) троянцы c) черви	ПК-1
17.	c	По «среде обитания» вирусы можно разделить на: a) не опасные b) очень опасные c) файловые	ПК-1
18.	c	Какие угрозы безопасности данных являются преднамеренными: a) ошибки персонала b) открытие электронного письма, содержащего вирус c) не авторизованный доступ	ПК-1

19.	c	По «среде обитания» вирусы можно разделить на: a) Опасные b) не опасные c) макровирусы	ПК-1
20.	c	Под какие системы распространение вирусов происходит наиболее динамично: a) Windows b) Mac OS c) Android	ПК-1
21.	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 c) заражают загрузочный сектор гибкого или жёсткого диска	ПК-1
22.	b	Какой вид идентификации и аутентификации получил наибольшее распространение: a) системы PKI b) постоянные пароли c) одноразовые пароли	ПК-1
24.	b	Для периодической проверки компьютера на наличие вирусов используется: a) Компиляция b) антивирусное сканирование c) дефрагментация диска	ПК-1

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 «**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).