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

Нестандартные методы защиты информации

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

Предисловие

1. Назначение: проведение текущего контроля успеваемости и промежуточной аттестации по дисциплине «Нестандартные методы защиты информации».

2. ФОС является приложением к программе дисциплины «Нестандартные методы защиты информации».

3. Разработчики:

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:
Бабенко М. Г.– зав. 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 рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Нестандартные методы защиты информации».
«___»_____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-9 Способен формировать требования к защите информации в автоматизированных системах				
Результаты обучения по дисциплине: *Индикатор:* **ИД-1$_{ПК-9}$** Обосновывает необходимость защиты информации в автоматизированной системе.	Не предоставляет отчет с обоснованием необходимости защиты информации в автоматизированной системе.	Предоставляет неполный отчет с обоснованием необходимости защиты информации в автоматизированной системе.	Предоставляет отчет с обоснованием необходимости защиты информации в автоматизированной системе.	Предоставляет детальный отчет с обоснованием необходимости защиты информации в автоматизированной системе.
Результаты обучения по дисциплине: *Индикатор:* **ИД-2$_{ПК-9}$** Определяет угрозы безопасности информации, обрабатываемой автоматизированной системой.	Не предоставляет отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой.	Предоставляет неполный отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой.	Предоставляет отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой.	Предоставляет детальный отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой.
Результаты обучения по дисциплине: *Индикатор:* **ИД-3$_{ПК-9}$** Разрабатывает архитектуру системы защиты информации автоматизированной системы.	Не предоставляет отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы.	Предоставляет неполный отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы.	Предоставляет отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы.	Предоставляет детальный отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы.
Результаты обучения по дисциплине: *Индикатор:*	Не предоставляет отчёт по результатам моделирования	Предоставляет неполный отчёт по результатам	Предоставляет отчёт по результатам моделирования	Предоставляет детальный отчёт по результатам моделирования

ИД-4$_{ПК-9}$ Моделирует защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.

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
		Семестр А	
1.	2	Что понимается под нестандартными методами защиты информации? 1. Использование межсетевых экранов и антивирусов 2. Методы, выходящие за рамки традиционных технических решений 3. Применение стандартов ISO/IEC 27001 4. Обычные способы шифрования данных	ПК-9
2.	4	Какой из методов относится к стеганографии? 1. RSA 2. Хеширование 3. Биометрия 4. Скрытие информации в изображении	ПК-9
3.	1	Что такое метод биометрической аутентификации? 1. Идентификация пользователя по физиологическим или поведенческим характеристикам 2. Проверка пароля в базе данных 3. Использование одноразовых токенов 4. Контроль MAC-адреса	ПК-9
4.	3	Какой метод можно отнести к психофизиологическим средствам защиты? 1. Электронная подпись 2. Криптографическое шифрование 3. Слежение за движением глаз и мимикой 4. Блокировка IP-адресов	ПК-9
5.	4	Что является целью применения методов социальной инженерии? 1. Защита от DDoS-атак 2. Шифрование конфиденциальной информации 3. Повышение отказоустойчивости системы 4. Получение доступа к информации через психологическое воздействие	ПК-9
6.	2	Какая из технологий позволяет реализовать поведенческую биометрию? 1. Отпечаток пальца 2. Анализ ритма набора текста	ПК-9

		3. Сканирование сетчатки глаза 4. Распознавание лица	
7.	1	Что позволяет достичь защита с помощью шумовых сигналов? 1. Скрытие полезной информации среди помех 2. Уничтожение носителей информации 3. Ускорение передачи данных 4. Выявление вторжений в систему	ПК-9
8.	3	Что из перечисленного является примером метода «ловушки» (honeypot)? 1. Роутер с фильтрацией IP 2. VPN-туннель 3. Вымышленный сервер, имитирующий уязвимую систему 4. Облачное хранилище с шифрованием	ПК-9
9.	4	Что является целью применения методов дезинформации? 1. Прямое уничтожение информации 2. Изоляция каналов связи 3. Запрет доступа к критическим файлам 4. Введение злоумышленника в заблуждение	ПК-9
10.	1	Что такое «обфускация» в программной защите? 1. Усложнение кода программы для затруднения анализа 2. Сжатие исполняемого файла 3. Снижение энергопотребления при вычислениях 4. Использование аппаратного ключа	ПК-9
11.	2	Что из нижеперечисленного относится к нестандартному программному методу защиты? 1. Установка антивируса 2. Защита путём запутывания логики выполнения кода 3. Аудит безопасности 4. Установка обновлений ОС	ПК-9
12.	3	Какая характеристика важна при применении методов поведенческой аутентификации? 1. IP-адрес устройства 2. Скорость передачи данных 3. Уникальность модели поведения пользователя 4. Размер файла с логами	ПК-9
13.	4	Какой из методов можно использовать для защиты от утечек информации через акустиче-	ПК-9

		ские каналы? 1. VPN 2. Брандмауэр 3. Антивирус 4. Генерация звукового шума в диапазоне человеческого слуха	
14.	1	Что представляет собой физическое уничтожение данных как метод защиты? 1. Полное разрушение носителя информации 2. Удаление файлов через стандартный интерфейс 3. Шифрование файлов 4. Хранение носителя в сейфе	ПК-9
15.	2	Какой подход используется в методе «запутывания маршрута» передачи информации? 1. Передача данных по одному выделенному каналу 2. Использование случайных промежуточных узлов 3. Сжатие данных перед отправкой 4. Защита канала с помощью TLS	ПК-9
16.	3	Что из нижеперечисленного является признаком атаки с использованием социальной инженерии? 1. Высокая нагрузка на сервер 2. Многочисленные ошибки аутентификации 3. Запрос доступа с формулировкой "от лица администратора" 4. Неудачные попытки расшифровки данных	ПК-9
17.	4	Какой из методов позволяет скрыть структуру программы от анализа? 1. Компрессия кода 2. Использование языков высокого уровня 3. Открытый исходный код 4. Применение полиморфного кода	ПК-9
18.	2	Что представляет собой метод «провокации атаки»? 1. Блокировка пользователя при подозрении 2. Создание условий для демонстрации поведения злоумышленника 3. Автоматическое шифрование данных 4. Контроль скорости передачи информации	ПК-9
19.	1	Что позволяет сделать метод «информационного насыщения»? 1. Усложнить извлечение полезной информации из большого объема данных	ПК-9

		2. Защитить пароли от перебора 3. Уменьшить размер логов 4. Повысить производительность сети	
20.	3	Какой из методов защиты относится к когнитивной безопасности? 1. Контроль доступа 2. Физическая охрана объекта 3. Противодействие манипуляциям с восприятием информации 4. Шифрование данных в памяти устройства	ПК-9

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).

.