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

Анализ уязвимостей программного обеспечения

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 «Анализ уязвимостей программного обеспечения». 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) «Анализ уязвимостей программного обеспечения»

3. Разработчик: Разработчик: Гусева Л.Л., доцент кафедры вычислительной математики и кибернетики

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

Рябцев С.С., старший преподаватель кафедры вычислительной математики и кибернетики

5. Представитель организации-работодателя: Березницкий А.С., заместитель директора ФБУ «Северо-Кавказский региональный центр судебной экспертизы Министерства юстиции РФ».

Экспертное заключение: Представленный ФОС по дисциплине «Анализ уязвимостей программного обеспечения» 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, а также целям и задачам рабочей программы реализуемой учебной дисциплины. Оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации представлены в полном объеме.

3. 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
Компетенция: **ПК-3**				
Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-2 ПК-3 выполняет анализ защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей	Имеет слабое представление о способах инструментального анализа защищенности компьютерной системы, сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей, осуществляет поиск уязвимостей и недокументированных возможностей программного обеспечения	Имеет частичное представление о способах инструментальнго анализа защищенности компьютерной системы, сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей, осуществляет поиск уязвимостей и недокументированных возможностей программного обеспечения	Имеет представление о способах инструментального анализа защищенности компьютерной системы, сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей, осуществляет поиск уязвимостей и недокументированных возможностей программного обеспечения	Имеет полное представление о способах инструментального анализа защищенности компьютерной системы, сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей, осуществляет поиск уязвимостей и недокументированных возможностей программного обеспечения
ИД-3 ПК-3	Имеет слабое	Имеет частичное	Имеет	Имеет полное

осуществляет поиск уязвимостей и недокументированных возможностей программного обеспечения	представление о методах поиска уязвимостей и недокументированных возможностей программного обеспечения	представление о методах поиска уязвимостей и недокументированных возможностей программного обеспечения	представление о методах поиска уязвимостей и недокументированных возможностей программного обеспечения	представление о методах поиска уязвимостей и недокументированных возможностей программного обеспечения
ПК-4				
Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-4 ПК-4 выявляет индивидуальные признаки программы, позволяющие впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы	Имеет слабое представление о методах проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов выявляет индивидуальные признаки программы, позволяющие впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы	Имеет частичное представление о методах проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов выявляет индивидуальные признаки программы, позволяющие впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы	Имеет представление о методах проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов выявляет индивидуальные признаки программы, позволяющие впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы	Имеет полное представление о методах проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов выявляет индивидуальные признаки программы, позволяющие впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы

Индикатор ИД-5 ПК-4 устанавливает участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация, устанавливает соответствия либо несоответствие действий с информацией специальному регламенту (правилам)	Имеет слабое представление о методах определения участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация, устанавливает соответствия либо несоответствие действий с информацией специальному регламенту (правилам)	Имеет частичное представление о методах определения участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация, устанавливает соответствия либо несоответствие действий с информацией специальному регламенту (правилам)	Имеет представление о методах определения участников события, их роли, места, условий, при которых была создана, модифицирова на или удалена информация, устанавливает соответствия либо несоответствие действий с информацией специальному регламенту (правилам)	Имеет полное представление о методах определения участников события, их роли, места, условий, при которых была создана, модифицирова на или удалена информация, устанавливает соответствия либо несоответствие действий с информацией специальному регламенту (правилам)

Оценочные средства для проверки уровня сформированности компетенций

Номер задания	**Правильный ответ**	**Содержание вопроса**	**Компетенция**
1	Выявление в коде программы, разработанной конкурирующей фирмой, интересные находки, которые в дальнейшем можно использовать в своих программах.	В чем заключается задача анализа программных реализаций? -Выявление в коде программы, разработанной -конкурирующей фирмой, интересные находки, которые в дальнейшем можно использовать в своих программах. -Выявление способов использования программы. -Сбор аналитических данных. -Оптимизация программ.	ПК-4
2	Отказ разработчиков от защиты своих программ от анализа.	Почему задача анализа программных реализаций является актуальной? • Отказ разработчиков от защиты своих программ от анализа. • Сложность разработки программ без анализа реализации. • Исследовательские требования.	ПК-4
3	В восстановлении алгоритма защиты посредством анализа имеющегося в распоряжении программного обеспечения.	В чем заключается статический метод анализа программ? • В восстановлении алгоритма защиты посредством анализа имеющегося в распоряжении программного обеспечения.	ПК-4

		• В восстановлении алгоритма защиты посредством использования статических данных. • В анализировании программы, похожей на имеющуюся.	
4	Метод экспериментов; статический метод; динамический метод.	Какие методы применяются для решения задачи анализа программных реализаций?	ПК-4
5	Аналитик угадывает алгоритмы преобразований.	Почему метод экспериментов с «черным ящиком» так называется?	ПК-4
6	Метод экспериментов с «черным ящиком» сводится к проведению по определенной методике многократных экспериментов (например, по зашифрованию различных текстов на различных ключах с помощью анализируемой системы криптографической защиты) и сравнительному анализу получаемых результатов (например, шифртекстов).	В чем состоит суть метода экспериментов с «черным ящиком»?	ПК-4
7	-все перечисленное выше верно	В чем заключаются достоинства и недостатки метода экспериментов с «черным ящиком»? - Нет гарантий, что угаданный результат соответствует действительности. - Метод приводит к успеху лишь в том случае, когда анализируемый алгоритм защиты достаточно прост. - В современных программных продуктах информация нередко записывается в сложном формате, который к тому же не документирован. - Часто входные данные программы содержат избыточную информацию, используемую для проверки их корректности. -все перечисленное выше верно	ПК-4
8	XOR SUB_256	Какие типичные эксперименты применяются при анализе программ методом экспериментов с «черным ящиком»?	ПК-4
9		Как определить наличие марканта в схеме шифрования архиватора ARJ?	ПК-3
10		Как восстановить схему шифрования, реализуемую архиватором ARJ?	ПК-3
11		На какие этапы разбивается решение задачи анализа программных реализаций?	ПК-3
12		Каковы достоинства и недостатки статического метода?	ПК-3
13		Какие проблемы возникают при дизассемблировании программных файлов?	ПК-3
14		Каковы типичные свойства «глупых»	ПК-3

		дизассемблеров?	
15		Каковы типичные свойства «умных» дизассемблеров?	ПК-3
16		Какие проблемы возникают при изучении аналитиком листингов дизассемблира?	ПК-3
17		Как осуществляется передача параметров в функции программ, написанных на C/C++?	ПК-3
18		Что такое Hex-Rays?	ПК-3
19		Что такое флаг трассировки?	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 если студент имеет полное представление о способах выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности, сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей

Оценка «хорошо» выставляется студенту в случае, когда студент имеет представление о способах выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности, сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей

Оценка «удовлетворительно» выставляется если студент имеет частичное представление о способах выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности, сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей

Оценка «неудовлетворительно» выставляется, если студент имеет слабое представление о способах выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности, сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей