

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Анатольевна

Должность: и.о. декана факультета математики и компьютерных наук имени

профессора Н.И. Червякова

Дата подписания: 22.09.2026 11:01:35

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619d42de79a7

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
Грובה Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Защита программ и данных

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

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Защита программ и 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 «Защита программ и данных»

3. Разработчик: Гусева Л.Л., 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:

Тебеева Ф.Б., профессор кафедры вычислительной математики и кибернетики

Осипов Д.Л., доцент кафедры вычислительной математики и кибернетики

Представитель организации-работодателя: Березницкий А.С., 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 «Защита программ и данных» соответствует требованиям ФГОС ВО. Предлагаемые преподавателем формы и средства текущего контроля адекватны целям и задачам реализации образовательной программы высшего образования по направлению подготовки 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.

5. Срок действия ФОС определяется сроком реализации образовательной программ

1. Описание показателей и критериев оценивания на различных этапах их формирования, описание шкал оценивания

Уровни сформированности компетенции(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 Способен проводить инструментальный анализ защищённости компьютерной системы и осуществлять поиск уязвимостей программного обеспечения				
Результаты обучения по дисциплине (модулю): Индикатор: ИД-2 ПК-3 выполняет анализ защищённости сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей	Имеет слабое представление о методах проведения анализа защищённости сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей	Имеет частичное представление о методах проведения анализа защищённости сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей	Имеет представление о методах проведения анализа защищённости сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей	Имеет полное представление о методах проведения анализа защищённости сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей
Результаты обучения по дисциплине (модулю): Индикатор: ИД-3 ПК-3 осуществляет поиск уязвимостей и недокументированных возможностей программного обеспечения	Имеет слабое представление о методах поиска уязвимостей и недокументированных возможностей программного обеспечения	Имеет частичное представление о методах поиска уязвимостей и недокументированных возможностей программного обеспечения	Имеет представление о методах поиска уязвимостей и недокументированных возможностей программного обеспечения	Имеет полное представление о методах поиска уязвимостей и недокументированных возможностей программного обеспечения
Компетенция: ПК-4 Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов				
Результаты обучения по дисциплине (модулю): Индикатор: ИД-3 ПК-4 выявляет индивидуальные признаки программы, позволяющие впоследствии идентифицировать её автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы	Имеет слабое представление о методах выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать её автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы	Имеет частичное представление о методах выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать её автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы	Имеет представление о методах выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать её автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы	Имеет полное представление о методах выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать её автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы
Результаты обучения по дисциплине (модулю): Индикатор: ИД-5 ПК-4 устанавливает	Имеет слабое представление о методах определения участников события, их ролей, мест и условий, при	Имеет частичное представление о методах определения участников события, их ролей, мест и условий, при	Имеет представление о методах определения участников события, их ролей, мест и условий, при	Имеет полное представление о методах определения участников события, их ролей, мест и условий, при

Уровни сформированности компетенции(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
участников события, их роли, места, условия, при которых была создана, модифицирована или удалена информация, устанавливает соответствие либо несоответствие действий с информацией специальному регламенту (правилам)	которых была создана, модифицирована или удалена информация, о порядке установления соответствия либо несоответствия действий с информацией специальному регламенту (правилам)	которых была создана, модифицирована или удалена информация, о порядке установления соответствия либо несоответствия действий с информацией специальному регламенту (правилам)	которых была создана, модифицирована или удалена информация, о порядке установления соответствия либо несоответствия действий с информацией специальному регламенту (правилам)	которых была создана, модифицирована или удалена информация, о порядке установления соответствия либо несоответствия действий с информацией специальному регламенту (правилам)

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1	Сбор детальной информации о функционировании какой-либо программы.	В чём заключается задача анализа программных реализаций? -: Сбор детальной информации о функционировании какой-либо программы. -: Изучение технической документации -: Анализ исходного кода -: Анализ уязвимостей	ПК-3
2	Статический метод; Динамический метод; Метод чёрного ящика	Какие методы применяются для решения задачи анализа программных реализаций? -: Метод экспериментов; -: Статический метод; -: Динамический метод; -: Метод чёрного ящика; -: Метод белого ящика	ПК-3
3	сверки времени	Инструкция rdtsc используется для: -: создания задержки отладки -: проверки контрольной суммы -: сверки времени	ПК-3
4	Всё перечисленное	Почему задача анализа программных реализаций является актуальной? -: Многообразие программных средств обработки информации и используемых в них средств защиты. -: Большой разброс в уровне подготовленности разработчиков. -: Широкое распространение программных средств зарубежного производства. -: Всё перечисленное	ПК-3
5	TLS	Вид хранилища в Windows, в котором объекты данных не являются автоматическими переменными стека, но принадлежат конкретному потоку, выполняющему код, называется: -: TLS -: TPR -: LPC	ПК-3
6		На какие этапы разбивается решение задачи анализа программных реализаций?	ПК-3
7	Метод экспериментов; Статический метод; Динамический метод	Какие методы применяются для решения задачи анализа программных реализаций?	ПК-3
8	Термин заимствован из математической теории автоматов	Почему метод экспериментов с «чёрным ящиком» так называется?	ПК-3
9	Проведению по определённой методике многократных экспериментов и сравнительному анализу получаемых результатов	В чём состоит суть метода экспериментов с «чёрным ящиком»?	ПК-3
10	Всё перечисленное	Недостатки метода экспериментов с «чёрным ящиком»?	ПК-4
11	Формат заголовков	Какие типичные примеры анализа программ	ПК-4

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
	бинарного файла данных.	методом «чёрного ящика» вам знакомы?	
12		Как определить наличие марканта в схеме шифрования архиватора arj?	ПК-4
13		Зашифровав с помощью arj несколько файлов на разных ключах, мы сразу обнаруживаем при визуальном просмотре полученных архивов, что файл архива включает в себя:	ПК-4
14		В чём заключается статический метод анализа защиты программ?	ПК-4
15		Что такое программные точки останова?	ПК-4
16	линейного дизассемблирования	Для какого алгоритма дизассемблирования характерна работа до достижения конца буфера, даже если инструкции управления потоком приводят к выполнению лишь небольшой части буфера?	ПК-4
17	добавлении после условных переходов байтов с данными	Методика дизассемблирования с добавлением ложного байта заключается в:	ПК-4
18	call	Какая из инструкций помещает в стек указатель на возвращаемое значение?	ПК-4
19	ret	Использование какой инструкции позволяет злоумышленникам затруднить дизассемблирование путём преждевременного завершения выполнения функции?	ПК-4
20	аппаратные точки останова	Для борьбы с методикой проверки контрольной суммы кода можно использовать: -: аппаратные точки останова -: ручное редактирование маршрута выполнения во время отладки программы	ПК-4

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость обучающихся по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний обучающихся основана на использовании совокупности контрольных мероприятий по проверке пройденного материала (контрольных точек), оптимально расположенных на всём временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний обучающихся 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 предусмотрена для обучающихся на образовательных программах уровня высшего образования магистратуры, а также для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной форм обучения.

3. Критерии оценивания компетенций

Оценивание проводится по компетенциям ПК-3 «Способен проводить инструментальный анализ защищённости компьютерной системы и осуществлять поиск уязвимостей программного обеспечения» и ПК-4 «Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов».

1. Оценка «отлично» выставляется обучающемуся, если он имеет полное представление о способах выполнения анализа защищённости компьютерных систем с использованием сканеров безопасности, о методах анализа сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей, о методах поиска уязвимостей и недокументированных возможностей программного обеспечения, а также о методах выявления индивидуальных признаков программы и установления участников события.

2. Оценка «хорошо» выставляется обучающемуся, если он имеет представление о перечисленных выше способах и методах, допуская отдельные неточности.

3. Оценка «удовлетворительно» выставляется обучающемуся, если он имеет частичное представление о перечисленных выше способах и методах.

4. Оценка «неудовлетворительно» выставляется обучающемуся, если он имеет слабое представление о перечисленных выше способах и методах.