

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: 19.06.2026 15:10:47

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619d42de79a7

**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
Грובה Т. А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
«Интеллектуальные методы анализа протоколов безопасности»

Направление подготовки
Профиль

02.04.01 Математика и компьютерные науки
Искусственный интеллект в
кибербезопасности

Год начала обучения
Форма обучения

2026
очная

Реализуется в 3 семестре

Введение

1. Назначение: Фонд оценочных средств предназначен для обеспечения методической основы для организации и проведения текущего контроля по дисциплине «Интеллектуальные методы анализа протоколов безопасности». 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 «Интеллектуальные методы анализа протоколов безопасности»

3. Разработчик: 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 направлению подготовки 02.04.01 Математика и компьютерные науки профиль «Искусственный интеллект в кибербезопасности» 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 (Неудовлетворит ельно) 2 балла	Минимальный уровень (удовлетворитель но) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
<i>Компетенция: ПК-8 Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники</i>				
Результаты обучения по дисциплине (модулю): <i>Индикатор: ИД-1. ПК-8.</i> участвует в межличностном и групповом взаимодействии, используя инклюзивный подход, эффективную коммуникацию, методы командообразования и командного взаимодействия при совместной работе в рамках поставленной задачи	не знает как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники	плохо знает как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники	знает как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники	отлично знает как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники
<i>ИД-2. ПК -8</i> обеспечивает работу команды для получения оптимальных результатов совместной работы, с учетом индивидуальных возможностей её членов, использования методологии достижения успеха, методов, информационных технологий и технологий форсайта	не умеет создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники	плохо умеет создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники	умеет создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники	отлично умеет создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники

ИД-3. ПК -8 обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения	не владеет как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники	плохо владеет как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники	владеет как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники	отлично владеет как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники
--	---	---	---	--

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.	Корректность RSA основана на взаимно обратных преобразованиях в кольце целых чисел по модулю $n=pq$, где p и q — простые числа. Доказательство корректности RSA включает в себя показ того, что $med \equiv m \pmod{n}$ для всех $m \in \mathbb{Z}_n$, что обеспечивается тем, что $ed \equiv 1 \pmod{\phi(n)}$	Доказать корректность систем шифрования RSA и Эль-Гамала.	ПК -8
2.	Доказательство корректности протоколов электронной подписи основывается на свойствах криптографических функций, таких как	Доказать корректность протоколов электронной подписи.	ПК -8

	необратимость и стойкость к подделке. Корректность достигается, если подпись может быть проверена только с использованием открытого ключа, соответствующего закрытому ключу, который использовался для подписи.		
3.	Доказательство отсутствия уязвимостей в протоколе обедающих криптографов может быть проведено с помощью формальных методов верификации, таких как анализ состояния системы и использование логических доказательств. При этом необходимо показать, что все участники могут безопасно обмениваться сообщениями, не подверженными атакам	Доказать отсутствие уязвимостей в протоколе обедающих криптографов.	ПК -8
4.	Обобщение протокола обедающих криптографов на произвольное	Построить обобщение протокола обедающих криптографов на случай произвольного количества участников и доказать его корректность и безопасность.	ПК -8

	количество участников может быть достигнуто путем применения многопользовательской аутентификации и распределенных ключей. Корректность и безопасность обобщенного протокола можно доказать, используя индукцию по количеству участников и методы анализа безопасности.		
5.	Доказательство корректности вероятностного алгоритма распознавания простоты чисел включает в себя анализ вероятностных свойств алгоритма, таких как вероятность ложного срабатывания. Корректность достигается, если для каждого простого числа алгоритм с высокой вероятностью возвращает "простое", а для составного числа — "составное".	Доказать корректность вероятностного алгоритма распознавания простоты чисел.	ПК -8

6.	Схема разделения секрета с заданным количеством групп может быть построена с использованием метода Шамира, где секрет делится на части, и для восстановления секрета требуется определенное количество частей. Это достигается путем использования полиномов и теоремы о интерполяции.	Построить схему разделения секрета с заданным количеством групп.	ПК -8
7.	Доказательство корректности протокола аутентификации на основе процессной модели требует формального анализа состояний и переходов в модели. Корректность достигается, если каждый участник может подтвердить свою идентичность, не раскрывая секретные данные.	Доказать корректность заданного протокола аутентификации на основе процессной модели.	ПК -8
8.	Доказательство корректности протокола передачи сообщений по	Доказать корректность протокола передачи сообщений по ненадежному каналу на основе процессной модели.	ПК -8

	ненадежному каналу основывается на анализе возможных состояний канала и обработке ошибок. Если протокол может успешно восстановить сообщение даже при наличии потерь и искажений, он считается корректным.		
9.	Построение протокола передачи сообщений по каналу с искажениями и потерей пакетов может включать использование методов контроля ошибок и подтверждения получения. Корректность достигается, если сообщения могут быть восстановлены и подтверждены получателями.	Построить протокол передачи сообщений по каналу с искажениями, потерей пакетов, дублированием и переупорядочением сообщений, и доказать его корректность.	ПК -8
10.	Доказательство корректности модифицированного протокола аутентификации Нидхэма-Шредера требует анализа его	Доказать корректность модифицированного протокола аутентификации Нидхэма-Шредера.	ПК -8

	устойчивости к атакам, таким как повторные атаки и атаки на подмену. Корректность подтверждается, если протокол обеспечивает уникальность и защищенность аутентификации для всех участников.		
11.	С	Какой из следующих методов используется для анализа криптографических протоколов? А) Верификация на основе конечных автоматов В) Проверка моделей С) Все вышеперечисленное D) Теоретико-доказательный подход	ПК -8
12.	В	Какая цель формальной верификации в контексте протоколов безопасности? А) Обеспечение быстрого выполнения протоколов В) Проверка соответствия протокола его формальному описанию С) Увеличение сложности протоколов D) Сокращение затрат на разработку	ПК -8
13.	С	Какой инструмент используется для символического моделирования и анализа протоколов безопасности? А) SPIN В) PRISM С) Tamarin Prover D) Frama-C	ПК -8
14.	В	Какой подход к верификации позволяет автоматически проверять выполнение заданных свойств безопасности? А) Теоретико-доказательный подход	ПК -8

		В) Проверка моделей С) Верификация на основе конечных автоматов D) Символьное выполнение	
15.	D	Какие преимущества обеспечивает формальная верификация в кибербезопасности? А) Надежные гарантии безопасности В) Увеличение скорости разработки С) Снижение затрат на тестирование D) Все вышеперечисленное	ПК -8
16.	B	Какой тип формальной верификации используется для проверки корректности параллельных программ? А) Верификация на основе конечных автоматов В) Проверка моделей С) Теоретико-доказательный подход D) Символьное выполнение	ПК -8
17.	B	Какой метод используется для анализа достижимости в протоколах безопасности? А) Верификация на основе конечных автоматов В) Проверка моделей С) Теоретико-доказательный подход D) Метод проверки типа	ПК -8
18.	A	Какой инструмент используется для формальной верификации свойств безопасности в программах на C? А) Frama-C В) SPIN С) PRISM D) Tamarin Prover	ПК -8
19.	B	Какой подход к верификации позволяет доказать отсутствие ошибок в программном коде?	ПК -8

		A) Проверка моделей B) Теоретико-доказательный подход C) Верификация на основе конечных автоматов D) Все вышеперечисленное	
20.	C	Какой тип логических формул часто используется для описания свойств безопасности протоколов? A) CTL (Computation Tree Logic) B) LTL (Linear Temporal Logic) C) Все вышеперечисленное D) Только CTL	ПК -8
21.	Формальная верификация обеспечивает надежные гарантии безопасности, позволяет выявлять уязвимости на ранних стадиях разработки и снижает затраты на тестирование и исправление ошибок	Опишите основные преимущества формальной верификации в контексте протоколов безопасности.	ПК -8
22.	SPIN, PRISM, NuSMV.	Какие инструменты используются для проверки моделей в анализе протоколов безопасности?	ПК -8
23.	Верификация на основе конечных автоматов — это метод, который моделирует поведение системы с помощью конечных автоматов для проверки ее свойств.	Что такое верификация на основе конечных автоматов, и как она применяется в анализе криптографических протоколов?	ПК -8

	В криптографии она используется для анализа протоколов аутентификации и обмена ключами.		
24.	Формальная верификация позволяет автоматически проверять соответствие протокола его формальному описанию, что помогает выявить потенциальные уязвимости и ошибки на ранних стадиях разработки	Как формальная верификация может помочь в выявлении уязвимостей в протоколах безопасности?	ПК -8
25.	Теоретико-доказательный подход позволяет строго доказать отсутствие ошибок в программном коде или протоколе, обеспечивая высокий уровень надежности и безопасности.	Опишите роль теоретико-доказательного подхода в формальной вери	ПК -8
26.	Нормализация протокола, определение свойств, выбор инструмента верификации, анализ результатов.	Опишите процесс формальной верификации криптографических протоколов и ее основные этапы.	ПК -8

27.	Формальные методы позволяют строго доказать корректность протоколов обмена ключами, проверяя свойства, такие как секретность и аутентификация. Это помогает выявить потенциальные уязвимости и улучшить протоколы	Как формальные методы могут быть использованы для анализа и улучшения безопасности протоколов обмена ключами?	ПК -8
28.	Проверка моделей позволяет быстро и автоматически проверять свойства протоколов, но может не охватывать все возможные состояния. Теоретико-доказательный подход обеспечивает строгие доказательства корректности, но требует значительных усилий и времени.	Сравните преимущества и недостатки проверки моделей и теоретико-доказательного подхода в контексте протоколов безопасности.	ПК -8
29.	Логические формализмы, такие как CTL и LTL, используются для описания свойств безопасности протоколов, таких как	Опишите применение логических формализмов (например, CTL, LTL) в анализе свойств безопасности протоколов.	ПК -8

	аутентификация и секретность. Они позволяют формализовать эти свойства и проверять их с помощью инструментов верификации.		
30.	Комбинированный подход, объединяющий проверку моделей и теоретико-доказательный метод, позволяет использовать сильные стороны каждого метода. Это обеспечивает как быстрое автоматическое тестирование, так и строгие доказательства корректности, что повышает эффективность анализа и надежность протоколов	Как комбинированный подход к верификации может улучшить эффективность анализа протоколов безопасности?	ПК -8

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 «отлично» выставляется студенту, если он, отлично знает как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, отлично умеет создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, отлично владеет как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники.

Оценка «хорошо» выставляется студенту, если он, умеет создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, владеет как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники.

Оценка «удовлетворительно» выставляется студенту, если он, плохо знает как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, плохо умеет создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, плохо владеет как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники.

Оценка «неудовлетворительно» выставляется студенту, если он, не знает как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, не умеет создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, не владеет как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники. Компетенция ПК-8 не освоена.