

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Грובה Татьяна Александровна
Должность: и.о. декана факультета математики и компьютерных наук имени
профессора Н.И. Червякова
Дата подписания: 17.06.2026 16:07:17
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
канд. физ. мат. наук, доцент Грובה Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по производственной практике
(вид практики: учебная/производственная)

Проектно-технологическая практика
(наименование (тип) практики)

Направление подготовки/специальность	10.04.01 «Информационная безопасность»
Направленность (профиль)/специализация	Информационная безопасность киберфизических систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	2

Введение

1. Назначение: Фонд оценочных средств (ФОС) предназначен для текущего контроля успеваемости и промежуточной аттестации по проектно-технологической практике студентов, обучающихся по направлению подготовки 10.04.01 «Информационная безопасность», направленность (профиль) «Информационная безопасность киберфизических систем».
2. ФОС является приложением к программе производственной практики, проектно-технологическая практика.
3. Разработчик (и) Бисюков В.М., доцент кафедры организации и технологии защиты информации
4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель: Петренко В.И., заведующий кафедрой организации и технологии защиты информации

Члены комиссии: Жук А.П., профессор кафедры организации и технологии защиты информации

Минкина Т.В., доцент кафедры организации и технологии защиты информации

Представитель организации-работодателя Демурчев Н.Г., директор ООО «Инфоком – С»

Экспертное заключение: Фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.04.01 «Информационная безопасность», направленность (профиль) «Информационная безопасность киберфизических систем» и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по производственной проектно-технологической практике.

5. Срок действия ФОС определяется сроком реализации образовательной программы

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

Компетенция(ИИ), индикатор (ы)	Уровни сформированности компетенции(ий)			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
ПК-3 Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем				
Результаты прохождения практики: Индикаторы: ПК-3 ИД-1 состав системы управления информационной безопасностью киберфизических систем	на низком уровне: знает состав, порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	в основном знает состав системы управления информационной безопасностью киберфизических систем	знает состав системы управления информационной безопасностью киберфизических систем	на высоком профессиональном уровне знает состав системы управления информационной безопасностью киберфизических систем
ПК-3 ИД-2 анализ уязвимости киберфизических систем	на низком уровне: умеет анализировать уязвимости киберфизических систем	в основном умеет анализировать уязвимости киберфизических систем	умеет анализировать уязвимости киберфизических систем	на высоком профессиональном уровне умеет анализировать уязвимости киберфизических систем
ПК-3 ИД-3 выбор набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем	на низком уровне владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем	в основном владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем	владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем	на высоком профессиональном уровне владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем
ПК-4 Способен оценивать уровень защищенности киберфизических систем и применять решения по обеспечению их информационной безопасности				
ПК-4 ИД-1 анализ структурно-функциональных характеристик	на низком уровне знает порядок структурно-	в основном знает порядок анализа структурно-	знает порядок анализа структурно-	на высоком профессиональном уровне знает порядок анализа

киберфизических систем	функциональных характеристик киберфизических систем	характеристик киберфизических систем	характеристик киберфизических систем	структурно-функциональных характеристик киберфизических систем
ПК- 4 ИД-2 выбор оптимального набора технических мер для повышения защищённости киберфизических систем	на низком уровне умеет выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем	в основном умеет выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем	умеет выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем	на высоком профессиональном уровне умеет выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем
ПК- 4 ИД-3 выбор организационно-технических мероприятия по обеспечению защиты киберфизических систем	на низком уровне владеет навыками выбора организационно-технических мероприятия по обеспечению защиты киберфизических систем	в основном владеет навыками выбора организационно-технических мероприятия по обеспечению защиты киберфизических систем	владеет навыками выбора организационно-технических мероприятия по обеспечению защиты киберфизических систем	на высоком профессиональном уровне владеет навыками выбора организационно-технических мероприятия по обеспечению защиты киберфизических систем

Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если студент на высоком уровне знает: состав системы управления информационной безопасностью киберфизических систем, порядок анализа структурно-функциональных характеристик киберфизических систем, умеет анализировать уязвимости киберфизических систем, выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем, владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем, выбора организационно-технических мероприятий по обеспечению защиты киберфизических систем.

Оценка «хорошо» выставляется студенту, если студент на хорошем уровне знает: состав системы управления информационной безопасностью киберфизических систем, порядок анализа структурно-функциональных характеристик киберфизических систем, умеет анализировать уязвимости киберфизических систем, выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем, владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем, выбора организационно-технических мероприятий по обеспечению защиты киберфизических систем.

Оценка «удовлетворительно» выставляется студенту, если студент на удовлетворительном уровне знает: состав системы управления информационной безопасностью киберфизических систем, порядок анализа структурно-функциональных характеристик киберфизических систем, умеет анализировать уязвимости киберфизических систем, выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем, владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем, выбора организационно-технических мероприятий по обеспечению защиты киберфизических систем.

Оценка «неудовлетворительно» выставляется студенту, если студент на низком уровне знает: состав системы управления информационной безопасностью киберфизических систем, порядок анализа структурно-функциональных характеристик киберфизических систем, умеет анализировать уязвимости киберфизических систем, выбирать оптимальный набор технических мер для повышения защищённости киберфизических систем, владеет навыками выбора набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем, выбора организационно-технических мероприятий по обеспечению защиты киберфизических систем.

2. Оценочные средства по производственной проектно-технологической практике

2.1. Задания, позволяющие оценить знания, полученные на практике

Формируемые компетенции, индикаторы		Формулировка задания
Код компетенции	Формулировка	
ПК-3	ПК-3 ИД-1 порядок функционирования и алгоритм построения системы управления информационной безопасностью	порядок построения алгоритм построения системы управления информационной безопасностью

	киберфизических систем	киберфизических систем
	ПК-3 ИД-2 анализ уязвимости и построение модели угроз для киберфизических систем	порядок анализа уязвимости и построение модели угроз для киберфизических систем
	ПК-3 ИД-3 выбор и реализация набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем	порядок выбора и реализация набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем
ПК-4	ПК- 4 ИД-1 анализ структурно-функциональных характеристик и определения уровня защищенности киберфизических систем	порядок анализа структурно-функциональных характеристик и определения уровня защищенности киберфизических систем
	ПК- 4 ИД-2 выбор оптимального набора мер для повышения защищённости киберфизических систем	порядок выбора оптимального набора мер для повышения защищённости киберфизических систем
	ПК- 4 ИД-3 выбор и реализация организационно-технических мероприятия по обеспечению защиты киберфизических систем	порядок выбора и реализации организационно-технических мероприятия по обеспечению защиты киберфизических систем

2.2. Задания, позволяющие оценить умения и навыки, полученные на практике

Формируемые компетенции, индикаторы		Формулировка задания
Код компетенции	Формулировка	
ПК-3	ПК-3 ИД-1 порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	построить алгоритм управления информационной безопасностью киберфизической системы
	ПК-3 ИД-2 анализ уязвимости и построение модели угроз для киберфизических систем	построить модель угроз для киберфизических систем
	ПК-3 ИД-3 выбор и реализация набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем	реализовать набор организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем
ПК-4	ПК- 4 ИД-1 анализ структурно-функциональных характеристик и определения уровня защищенности киберфизических систем	определить уровень защищенности киберфизической системы
	ПК- 4 ИД-2 выбор оптимального набора мер для повышения защищённости киберфизических систем	выбрать оптимальный набор мер для повышения защищённости киберфизических систем
	ПК- 4 ИД-3 выбор и реализация организационно-технических мероприятия по обеспечению защиты киберфизических систем	реализовать организационно-технические мероприятия по обеспечению защиты киберфизических систем

3. Методические материалы, определяющие процедуры оценивания и характеризующих этапы формирования компетенций

Процедура прохождения практики включает в себя следующие этапы

Разделы (этапы) практики	Реализуемые компетенции / индикаторы	Виды производственной работы на практике, включая самостоятельную работу студентов	Трудоемкость (час.)	Формы текущего контроля
--------------------------	--------------------------------------	--	---------------------	-------------------------

Подготовительный	ПК-3	проектно-технологическая лекция, инструктаж по технике безопасности	16	Письменный отчет
Исследовательский этап	ПК-4	сбор, обработка и систематизация фактического и литературного материала	40	Письменный отчет
Этап обработки и анализа информации	ПК-3, ПК-4	наблюдения, измерения, выполнение индивидуального задания	80	Письменный отчет
Итоговый этап	ПК-3, ПК-4	анализ, обработка и систематизация материала, подготовка отчёта	80	собеседование, письменный отчет
Итого			216	

На каждом этапе практики осуществляется текущий контроль за процессом формирования компетенций. Предлагаемые студенту задания позволяют проверить компетенции: ПК-3, ПК-4.

Форма и вид отчетности студентов о прохождении практики определяются в рабочей программе практики. По результатам прохождения практики студент представляет руководителю практики от кафедры следующие отчетные документы, заверенные подписью руководителя от организации-базы практики:

- отчет,
- отзыв руководителем практики от профильной организации или структурного подразделения СКФУ в случае, когда практика проводится на базе Университета.

Отчёт по практике включает:

- задание на практику,
- календарный план прохождения практики и краткое описание ежедневных видов работ, выполненных практикантам,
- участие в научно-исследовательской работе, краткое описание работы (при наличии),
- занятия, проводимые на практике,
- участие в экскурсиях,
- полученная рабочая профессия (при необходимости),
- анкета обучающегося по итогам практики.

По окончании практики студент составляет письменный отчет. Отчет проверяется и подписывается непосредственным руководителем практики от Университета и руководителем практики от профильной организации. Подпись руководителя практики от профильной организации должна быть заверена печатью организации. Содержание и оформление отчета должны соответствовать требованиям, разработанным выпускающей кафедрой. Информационные блоки отчета должны быть представлены в следующем порядке:

1. Титульный лист.
2. Содержание.
3. Введение (цели и задачи практики, краткая характеристика базы и места практики, описание основных видов деятельности, выполняемых практикантом).
4. Разделы и подразделы (сведения о конкретно выполненной студентом работе в период практики в соответствии с заданием или описание деятельности, выполняемой в процессе прохождения практики, достигнутые результаты).
5. Заключение (выводы о результатах практики и анализ возникших проблем)
6. Список использованных источников.

7. Приложения (по необходимости).

Оценка по практике учитывает качество представленных студентом отчетных материалов и отзывы (характеристики) руководителей практики.

При проверке заданий, оцениваются:

- последовательность и рациональность выполнения задания,
- логичность изложения,
- полнота описания.

При проверке отчетов оцениваются

- самостоятельность выполнения задания,
- качество оформления и представления результатов работы,
- уровень защиты и ответов на вопросы.

При защите отчета оцениваются:

- самостоятельность выполнения задания,
- качество оформления и представления результатов работы,
- уровень защиты и ответов на вопросы.