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 Гробова Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по производственной практике

(вид практики: учебная/производственная)

Эксплуатационная 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	4

Введение

1. Назначение: Фонд оценочных средств (ФОС) предназначен для текущего контроля успеваемости и промежуточной аттестации по эксплуатационной 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, эксплуатационная 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 эксплуатационной 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-2 Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах				
Результаты прохождения практики: Индикаторы: ПК-2 ИД-1 разрабатывает политику безопасности в киберфизических системах	на низком уровне знает состав, назначение и порядок разработки политики безопасности в киберфизических системах,	в основном знает состав, назначение и порядок разработки политики безопасности в киберфизических системах,	знает состав, назначение и порядок разработки политики безопасности в киберфизических системах,	на высоком профессиональном уровне знает состав, назначение и порядок разработки политики безопасности в киберфизических системах
ПК-2 ИД-2 проектирует политику безопасности вычислительных сетей в киберфизических системах	на низком уровне умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах	в основном умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах	умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах	на высоком профессиональном уровне умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах
ПК-2 ИД-3 реализует комплекс выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	на низком уровне владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	в основном владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	на высоком профессиональном уровне владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах
ПК-4 Способен к формированию требований к защите информации в автоматизированных системах				
ПК-4 ИД-1 анализирует	с грубыми ошибками применяет	в основном применяет	применяет основные	в полном объёме применяет

характер обрабатываемой информации и определяет перечень информации, подлежащей защите, выявляет степени участия персонала в обработке защищаемой информации, планирует мероприятия по обеспечению защиты информации в автоматизированной системе	основные информационные технологии, угрозы безопасности информации и модели нарушителя в автоматизированных системах, анализирует цели создания автоматизированных систем и задачи, решаемые автоматизированными системами, выявляет уязвимости информационно-технологических ресурсов автоматизированных систем, определяет угрозы безопасности информации, обрабатываемой автоматизированной системой	основные информационные технологии, угрозы безопасности информации и модели нарушителя в автоматизированных системах, анализирует цели создания автоматизированных систем и задачи, решаемые автоматизированными системами, выявляет уязвимости информационно-технологических ресурсов автоматизированных систем, определяет угрозы безопасности информации, обрабатываемой автоматизированной системой	информационные технологии, угрозы безопасности информации и модели нарушителя в автоматизированных системах, анализирует цели создания автоматизированных систем и задачи, решаемые автоматизированными системами, выявляет уязвимости информационно-технологических ресурсов автоматизированных систем, определяет угрозы безопасности информации, обрабатываемой автоматизированной системой	основные информационные технологии, угрозы безопасности информации и модели нарушителя в автоматизированных системах, анализирует цели создания автоматизированных систем и задачи, решаемые автоматизированными системами, выявляет уязвимости информационно-технологических ресурсов автоматизированных систем, определяет угрозы безопасности информации, обрабатываемой автоматизированной системой
ПК-4 ИД-2 определяет требуемый класса (уровень) защищенности автоматизированной системы, обосновывает необходимости использования криптографических средств защиты информации, разрабатывает отчетные документы и разделы технических заданий	с грубыми ошибками определяет виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах, методы защиты информации от «утечки» по техническим каналам, моделирует защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	в основном определяет виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах, методы защиты информации от «утечки» по техническим каналам, моделирует защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	определяет виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах, методы защиты информации от «утечки» по техническим каналам, моделирует защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	в полном объёме определяет виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах, методы защиты информации от «утечки» по техническим каналам, моделирует защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации

Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если студент на высоком уровне знает состав, назначение и порядок разработки политики безопасности в киберфизических системах, порядок определения уровня защищенности киберфизических систем, умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах, выбирать оптимальный набор организационных мер для повышения защищённости киберфизических систем, владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах, навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем.

Оценка «хорошо» выставляется студенту, если студент на хорошем уровне знает состав, назначение и порядок разработки политики безопасности в киберфизических системах, порядок определения уровня защищенности киберфизических систем, умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах, выбирать оптимальный набор организационных мер для повышения защищённости киберфизических систем, владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах, навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем.

Оценка «удовлетворительно» выставляется студенту, если студент на удовлетворительном уровне знает состав, назначение и порядок разработки политики безопасности в киберфизических системах, порядок определения уровня защищенности киберфизических систем, умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах, выбирать оптимальный набор организационных мер для повышения защищённости киберфизических систем, владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах, навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем.

Оценка «неудовлетворительно» выставляется студенту, если студент на низком уровне знает состав, назначение и порядок разработки политики безопасности в киберфизических системах, порядок определения уровня защищенности киберфизических систем, умеет применять современные информационные технологии, при проектировании политики безопасности вычислительных сетей в киберфизических системах, выбирать оптимальный набор организационных мер для повышения защищённости киберфизических систем, владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах, навыками реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем.

2. Оценочные средства по производственной эксплуатационной практике

2.1 Задания, позволяющие оценить знания, полученные на практике

Формируемые компетенции, индикаторы		Формулировка задания
Код компетенции	Формулировки	
ПК-2	ПК-2 ИД-1 разрабатывает политику безопасности в киберфизических системах	порядок разработки политики безопасности в киберфизических системах
	ПК-2 ИД-2 проектирует политику безопасности вычислительных сетей в киберфизических системах	порядок разработки политики безопасности в вычислительных сетях
	ПК-2 ИД-3 комплекс выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	порядок выбора комплекса мер, при реализации политики безопасности вычислительных сетей в киберфизических системах
ПК-4	ПК-4 ИД-1 порядок определения уровня защищенности киберфизических систем	порядок определения уровня защищенности киберфизических систем
	ПК-4 ИД-2 выбор оптимального набора организационных мер для повышения защищённости киберфизических систем	порядок выбора оптимального набора организационных мер для повышения защищённости киберфизических систем
	ПК-4 ИД-3 реализация организационно-технических мероприятия по обеспечению защиты киберфизических систем	порядок реализации организационно-технических мероприятий по обеспечению защиты киберфизических систем

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

Формируемые компетенции, индикаторы		Формулировка задания
Код компетенции	Формулировки	
ПК-2	ПК-2 ИД-1 разрабатывает политику безопасности в киберфизических системах	разработать политику безопасности в киберфизической системе
	ПК-2 ИД-2 проектирует политику безопасности вычислительных сетей в киберфизических системах	разработать политику безопасности в вычислительной сети
	ПК-2 ИД-3 комплекс выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	выбрать комплекс мер, для реализации политики безопасности вычислительных сетей в киберфизических системах
ПК-4	ПК-4 ИД-1 порядок определения уровня защищенности киберфизических систем	определить уровень защищенности киберфизической системы
	ПК-4 ИД-2 выбор оптимального набора организационных мер для повышения защищённости киберфизических систем	выбрать оптимальныйо набор организационных мер для защиты киберфизической системы
	ПК-4 ИД-3 реализация организационно-технических мероприятия по обеспечению защиты киберфизических систем	реализовать организационно-технические мероприятия по обеспечению защиты киберфизической системы

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	ПК2, ПК-4	Ознакомительный, инструктаж по технике безопасности	80	Письменный отчет
Исследовательский этап	ПК-2, ПК-4	сбор, обработка и систематизация фактического и литературного материала	100	Письменный отчет
Этап обработки и анализа информации	ПК-2, ПК-4	наблюдения, измерения, выполнение индивидуального задания	100	Письменный отчет
Итоговый этап	ПК-2, ПК-4	анализ, обработка и систематизация материала, подготовка отчёта	44	собеседование, письменный отчет
		Итого	324	

На каждом этапе практики осуществляется текущий контроль за процессом формирования компетенций. Предлагаемые студенту задания позволяют проверить компетенции: ПК-2, 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 литературы.

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.