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	10.03.01 «Информационная безопасность»
Направленность (профиль)/специализация	Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	8

Введение

1. Назначение: Фонд оценочных средств (ФОС) предназначен для текущего контроля успеваемости и промежуточной аттестации по эксплуатационной практике студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

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 «СГУ-Инфоком»

Экспертное заключение: Фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» 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 администрировать средства защиты информации в компьютерных системах и сетях Способен администрировать средства защиты информации в компьютерных системах и сетях				
Результаты прохождения практики: Индикатор: ИД-1 ПК-2 определяет состав применяемых программно-аппаратных средств защиты информации в операционных системах, разрабатывает порядок применения программно-аппаратных средств зашиты информации в операционных системах	на низком уровне определяет архитектуру и принципы построения операционных систем, программные интерфейсы операционных систем, формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах	в основном определяет архитектуру и принципы построения операционных систем, программные интерфейсы операционных систем, формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах	определяет архитектуру и принципы построения операционных систем, программные интерфейсы операционных систем, формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах	в полном объёме определяет архитектуру и принципы построения операционных систем, программные интерфейсы операционных систем, формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах
ИД-2 ПК-2 устанавливает программно-аппаратные средства защиты информации в операционных системах, включая средства криптографической защиты информации, конфигурирует программно-аппаратные средства защиты информации в	на низком уровне определяет порядок контроля корректности функционирования программно-аппаратных средств защиты информации в операционных системах, управляет антивирусной защитой операционных систем в соответствии с действующими требованиями	в основном определяет порядок контроля корректности функционирования программно-аппаратных средств защиты информации в операционных системах, управляет антивирусной защитой операционных систем в соответствии с действующими	определяет порядок контроля корректности функционирования программно-аппаратных средств защиты информации в операционных системах, управляет антивирусной защитой операционных систем в соответствии с действующими требованиями	в полном объёме определяет порядок контроля корректности функционирования программно-аппаратных средств защиты информации в операционных системах, управляет антивирусной защитой операционных систем в соответствии с действующими требованиями

операционных системах		требованиями		
ПК-3 Способен обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации				
ИД-1 ПК-3 обнаруживает инциденты в процессе эксплуатации автоматизированной системы, проводит их идентификацию, оценивает защищенность автоматизированных систем с помощью типовых программных средств, определяет источники и причины возникновения инцидентов, оценивает последствия выявленных инцидентов	на низком уровне определяет нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации, источники и причины возникновения инцидентов, проводит оценивание последствий выявленных инцидентов	в основном определяет нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации, источники и причины возникновения инцидентов, проводит оценивание последствий выявленных инцидентов	определяет нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации, источники и причины возникновения инцидентов, проводит оценивание последствий выявленных инцидентов	в полном объёме определяет нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации, источники и причины возникновения инцидентов, проводит оценивание последствий выявленных инцидентов
ИД-2 ПК-3 осуществляет инструментальный контроль и расчёты показателей эффективности защиты информации, обрабатываемой в автоматизированных системах, обнаруживает нарушения правил разграничения доступа	на низком уровне определяет организационные меры по защите информации, принципы построения средств защиты информации от «утечки» по техническим каналам, критерии оценки защищенности автоматизированной системы, применяет технические средства контроля эффективности мер защиты информации	в основном определяет организационные меры по защите информации, принципы построения средств защиты информации от «утечки» по техническим каналам, критерии оценки защищенности автоматизированной системы, применяет технические средства контроля эффективности мер защиты информации	определяет организационные меры по защите информации, принципы построения средств защиты информации от «утечки» по техническим каналам, критерии оценки защищенности автоматизированной системы, применяет технические средства контроля эффективности мер защиты информации	в полном объёме определяет организационные меры по защите информации, принципы построения средств защиты информации от «утечки» по техническим каналам, критерии оценки защищенности автоматизированной системы, применяет технические средства контроля эффективности мер защиты информации

Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если студент в полном объёме знает архитектуру и принципы построения операционных систем, программные интерфейсы операционных систем, порядок контроля корректности функционирования программно-аппаратных средств защиты информации в операционных системах, нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации, организационные меры по защите информации, принципы построения средств защиты информации от «утечки» по техническим каналам, критерии оценки защищенности автоматизированной системы, умеет применять технические средства контроля эффективности мер защиты информации, управлять антивирусной защитой операционных систем в соответствии с действующими требованиями, определять источники и причины возникновения инцидентов, проводит и оценивать последствия выявленных инцидентов, формировать шаблоны установки программно-аппаратных средств защиты информации в операционных системах.

Оценка «хорошо» выставляется студенту, если студент знает архитектуру и принципы построения операционных систем, программные интерфейсы операционных систем, порядок контроля корректности функционирования программно-аппаратных средств защиты информации в операционных системах, нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации, организационные меры по защите информации, принципы построения средств защиты информации от «утечки» по техническим каналам, критерии оценки защищенности автоматизированной системы, умеет применять технические средства контроля эффективности мер защиты информации, управлять антивирусной защитой операционных систем в соответствии с действующими требованиями, определять источники и причины возникновения инцидентов, проводит и оценивать последствия выявленных инцидентов, формировать шаблоны установки программно-аппаратных средств защиты информации в операционных системах.

Оценка «удовлетворительно» выставляется студенту, если студент в основном знает архитектуру и принципы построения операционных систем, программные интерфейсы операционных систем, порядок контроля корректности функционирования программно-аппаратных средств защиты информации в операционных системах, нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации, организационные меры по защите информации, принципы построения средств защиты информации от «утечки» по техническим каналам, критерии оценки защищенности автоматизированной системы, умеет применять технические средства контроля эффективности мер защиты информации, управлять антивирусной защитой операционных систем в соответствии с действующими требованиями, определять источники и причины возникновения инцидентов, проводит и оценивать последствия выявленных инцидентов, формировать шаблоны установки программно-аппаратных средств защиты информации в операционных системах.

Оценка «неудовлетворительно» выставляется студенту, если студент на низком уровне знает архитектуру и принципы построения операционных систем, программные интерфейсы операционных систем, порядок контроля корректности функционирования программно-аппаратных средств защиты информации в операционных системах, нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации, организационные меры по защите информации, принципы построения средств защиты информации от «утечки» по

техническим каналам, критерии оценки защищенности автоматизированной системы, умеет применять технические средства контроля эффективности мер защиты информации, управлять антивирусной защитой операционных систем в соответствии с действующими требованиями, определять источники и причины возникновения инцидентов, проводит и оценивать последствия выявленных инцидентов, формировать шаблоны установки программно-аппаратных средств защиты информации в операционных системах

2. Оценочные средства по эксплуатационной практике

2.1. Задания, позволяющие оценить знания, полученные на практике

Формируемые компетенции, индикаторы		Формулировка задания
Код компетенции	Формулировка	
ПК-2	Способен администрировать средства защиты информации в компьютерных системах и сетях Способен администрировать средства защиты информации в компьютерных системах и сетях	перечень нормативно - правовых актов, регламентирующих систему защиты информации
		нормативно - правовые акты ФСТЭК по ИБ
		нормативно - правовые акты ФСБ по ИБ
ПК-3	Способен обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации	перечень ситуаций, при которых необходимо оказывать первую помощь
		методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций
		мероприятия по охране труда и технике безопасности

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

Формируемые компетенции, индикаторы		Формулировка задания
Код компетенции	Формулировка	
ПК-2	Способен администрировать средства защиты информации в компьютерных системах и сетях Способен администрировать средства защиты информации в компьютерных системах и сетях	Порядок проведения анализа результатов эксперимента
		Перечень информационных активов предприятия.
		Какие виды и формы информации могут быть подвержены угрозам
ПК-3	Способен обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации	Виды, возможные методы и пути реализации угроз информационным ресурсам.
		Какова организационно-штатная структура подразделений, занимающихся вопросами обеспечения ИБ на предприятии
		Перечислить стандарты, регламентирующие ИБ

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

Этапы прохождения эксплуатационной практики, реализуемые компетенции, время, отводимое на каждый этап, а также формы контроля представлены в таблице

Разделы (этапы) практики	Реализуемые компетенции /	Виды учебной работы на практике, включая	Трудоемкость	Формы текущего

	индикаторы	самостоятельную работу студентов	(час.)	контроля
Подготовительный	ПК-2, ПК-3	ознакомительная лекция, инструктаж по технике безопасности	20	Письменный отчет
Исследовательский этап	ПК-2, ПК-3	сбор, обработка и систематизация фактического и литературного материала	40	Письменный отчет
Этап обработки и анализа информации	ПК-2, ПК-3	наблюдения, измерения, выполнение индивидуального задания	40	Письменный отчет
Итоговый этап	ПК-2, ПК-3	анализ, обработка и систематизация материала, подготовка отчёта	8	собеседование, письменный отчет
		Итого	108	

На каждом этапе практики осуществляется текущий контроль за процессом формирования компетенций. Предлагаемые студенту задания позволяют проверить компетенции: ПК-2, ПК-3.

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.