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
Гробова Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ «Разработка и эксплуатация автоматизированных систем в защищённом исполнении»

Специальность	Информационная безопасность автоматизированных систем
Направленность (профиль)	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	А

Предисловие

1. Назначение: проведение текущего контроля успеваемости и промежуточной аттестации по дисциплине «Разработка и эксплуатация автоматизированных систем в защищённом исполнении». 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 «Разработка и эксплуатация автоматизированных систем в защищённом исполнении».

3. Разработчики: Пастух С.А., - доцент кафедры вычислительной математики и кибернетики

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:
Бабенко М. Г.– зав. 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 специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» 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 (неудовлетворительно) 2 балла	**Минимальный уровень (удовлетворительно) 3 балла**	**Средний уровень (хорошо) 4 балла**	**Высокий уровень (отлично) 5 баллов**
Компетенция: **ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем**				
Результаты обучения по дисциплине: *Индикатор:* **ИД-1опк-11** Использует методологический базис теории защиты информации, используемый при разработке программно-аппаратных компонентов комплексных систем обеспечения информационной безопасности.	Не предоставляет отчет, с полным пояснением, в котором демонстрирует навык использования методологического базиса теории защиты информации, используемый при разработке программно-аппаратных компонентов комплексных систем обеспечения информационной безопасности.	Предоставляет неполный отчет с полным пояснением, в котором демонстрирует навык использования методологического базиса теории защиты информации, используемый при разработке программно-аппаратных компонентов комплексных систем обеспечения информационной безопасности.	Предоставляет отчет, с полным пояснением, в котором демонстрирует навык использования методологического базиса теории защиты информации, используемый при разработке программно-аппаратных компонентов комплексных систем обеспечения информационной безопасности.	Предоставляет детальный отчет с полным пояснением, в котором демонстрирует навык использования методологического базиса теории защиты информации, используемый при разработке программно-аппаратных компонентов комплексных систем обеспечения информационной безопасности.
Результаты обучения по дисциплине: *Индикатор:* **ИД-2опк-11** Осуществляет отбор и систематизацию компоненто	Не предоставляет отчет, где демонстрирует способность разрабатывать компоненты комплексных систем защиты информации	Предоставляет неполный отчет где демонстрирует способность разрабатывать компоненты комплексных	Предоставляет отчет, где демонстрирует способность разрабатывать компоненты комплексных систем защиты информации автоматизиров	Предоставляет детальный отчет, где демонстрирует способность разрабатывать компоненты комплексных систем защиты информации

в комплексных систем защиты информации автоматизированных систем.	автоматизированных систем.	систем защиты информации автоматизированных систем.	анных систем.	автоматизированных систем.
Результаты обучения по дисциплине: *Индикатор:* **ИД-3опк-11** Разрабатывает компоненты комплексных систем защиты информации автоматизированных систем	Не предоставляет отчет, где демонстрирует способность разрабатывать компоненты комплексных систем защиты информации автоматизированных систем.	Предоставляет неполный отчет где демонстрирует способность разрабатывать компоненты комплексных систем защиты информации автоматизированных систем.	Предоставляет отчет, где демонстрирует способность разрабатывать компоненты комплексных систем защиты информации автоматизированных систем.	Предоставляет детальный отчет, где демонстрирует способность разрабатывать компоненты комплексных систем защиты информации автоматизированных систем.
Компетенция: **ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений**				
Результаты обучения по дисциплине: *Индикатор:* **ИД-1опк-14** Использует: - основные принципы организации технического, программного обеспечения защищенных информационных систем; - основные принципы оптимального	Не предоставляет отчет в котором демонстрирует умение применять основные принципы организации технического, программного обеспечения защищенных информационных систем; основные принципы оптимального проектирования защищенных информационных систем и	Предоставляет неполный отчет в котором демонстрирует умение применять основные принципы организации технического, программного обеспечения защищенных информационных систем; основные принципы оптимального проектирован	Предоставляет отчет в котором демонстрирует умение применять основные принципы организации технического, программного обеспечения защищенных информационных систем; основные принципы оптимального проектирования защищенных информационных систем и основные	Предоставляет детальный отчет в котором демонстрирует умение применять основные принципы организации технического, программного обеспечения защищенных информационных систем; основные принципы оптимального проектирования защищенных информационных систем и основные

проектирования защищенных информационных систем; - основные принципы оценки показателей эффективности защищенных информационных систем.	основные принципы оценки показателей эффективности защищенных информационных систем	ия защищенных информационных систем и основные принципы оценки показателей эффективности защищенных информационных систем	принципы оценки показателей эффективности защищенных информационных систем	принципы оценки показателей эффективности защищенных информационных систем
Результаты обучения по дисциплине: *Индикатор:* **ИД-2ОПК-14** Осуществляет разработку проектных решений систем защиты, оформляет проектную документацию; использует методы оптимального проектирования, защищенных информационных и телекоммуникационных систем; проводит методы оценки эффективности, надежности, отказоустойчивости и производительности решений по обеспечению	Не предоставляет отчет в котором демонстрирует способность осуществлять разработку проектных решений систем защиты, оформлять проектную документацию; использовать методы оптимального проектирования, защищенных информационных и телекоммуникационных систем, а также проводить методы	Предоставляет неполный отчет с неполным пояснением в котором демонстрирует способность осуществлять разработку проектных решений систем защиты, оформлять проектную документацию; использовать методы оптимального проектирования, защищенных информационных и телекоммуникационных систем, а также проводить	Предоставляет отчет с пояснением в котором демонстрирует способность осуществлять разработку проектных решений систем защиты, оформлять проектную документацию; использовать методы оптимального проектирования, защищенных информационных и телекоммуникационных систем, а также проводить методы оценки эффективности, надежности, отказоустойчивости и	Предоставляет детальный отчет с полным пояснением в котором демонстрирует способность осуществлять разработку проектных решений систем защиты, оформлять проектную документацию; использовать методы оптимального проектирования, защищенных информационных и телекоммуникационных систем, а так же проводить методы оценки эффективности, надежности, отказоустойчивости и производительности решений

защищенности информационных и телекоммуникационных систем.		методы оценки эффективности, надежности, отказоустойчивости и производительности решений по обеспечению защищенности информационных и телекоммуникационных систем.	производительности решений по обеспечению защищенности информационных и телекоммуникационных систем.	по обеспечению защищенности информационных и телекоммуникационных систем.
Результаты обучения по дисциплине: *Индикатор:* **ИД-З$_{ОПК-14}$** Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем в защищенном исполнении с учетом требований по защите информации.	Не предоставляет отчет, в котором демонстрирует способность осуществлять разработку, внедрение и эксплуатацию автоматизированных систем в защищенном исполнении с учетом требований по защите информации.	Предоставляет неполный отчет, в котором демонстрирует способность осуществлять разработку, внедрение и эксплуатацию автоматизированных систем в защищенном исполнении с учетом требований по защите информации.	Предоставляет отчет, в котором демонстрирует способность осуществлять разработку, внедрение и эксплуатацию автоматизированных систем в защищенном исполнении с учетом требований по защите информации.	Предоставляет детальный отчет, в котором демонстрирует способность осуществлять разработку, внедрение и эксплуатацию автоматизированных систем в защищенном исполнении с учетом требований по защите информации.
Компетенция: **ОПК-7.2. Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации**				

Результаты обучения по дисциплине: *Индикатор:* **ИД-1опк-7.2** Осуществляет разработку проектных и организационных решений.	Не предоставляет отчет, где демонстрирует способность осуществлять разработку проектных и организационных решений	Предоставляет неполный отчет, где демонстрирует способность осуществлять разработку проектных и организационных решений	Предоставляет отчет, где демонстрирует способность осуществлять разработку проектных и организационных решений	Предоставляет детальный отчет, где демонстрирует способность осуществлять разработку проектных и организационных решений
Результаты обучения по дисциплине: *Индикатор:* **ИД-2опк-7.2** Формулирует требования к информационным системам в соответствии с нормативными требованиями к этим системам.	Не предоставляет отчет, где демонстрирует способность формировать требования к автоматизированным системам в защищенном исполнении	Предоставляет неполный отчет, где демонстрирует способность формировать требования к автоматизированным системам в защищенном исполнении	Предоставляет отчет, где демонстрирует способность формировать требования к автоматизированным системам в защищенном исполнении	Предоставляет детальный отчет, где демонстрирует способность формировать требования к автоматизированным системам в защищенном исполнении
Результаты обучения по дисциплине: *Индикатор:* **ИД-3опк-7.2** Способен осуществлять администрирование и контроль функционировании информационной системы и формировать исходные требования к	Не предоставляет отчет, где демонстрирует способность осуществлять администрирование и контроль функционирования автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе,	Предоставляет неполный отчет, где демонстрирует способность осуществлять администрирование и контроль функционирования автоматизированной системы в защищенном исполнении и формировать исходные	Предоставляет отчет, где демонстрирует способность осуществлять администрирование и контроль функционирования автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее	Предоставляет детальный отчет, где демонстрирует способность осуществлять администрирование и контроль функционирования автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее

этой системе, процессу ее создания и эксплуатации.	процессу ее создания и эксплуатации.	требования к этой системе, процессу ее создания и эксплуатации.	создания и эксплуатации.	создания и эксплуатации.

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
		Семестр А	
1.	c	Как называется автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или иных нормативных документов по защите информации? a) государственная автоматизированная система b) автоматизированная система обработки персональных данных c) автоматизированная система в защищенном исполнении d) объект информатизации	ОПК-11, ОПК - 14, ОПК -7.2
2.	b	В соответствии с ГОСТ Р 51583-2014 формирование требований к системе защиты информации АСЗИ осуществляется: a) разработчиком СЗИ АСЗИ b) обладателем информации (заказчиком) c) ФСТЭК d) ФСБ	ОПК-11, ОПК - 14, ОПК -7.2
3.	b	Какой ГОСТ определяет порядок создания системы защиты информации автоматизированной системы в защищенном исполнении? a) ГОСТ Р 50922-2006 b) ГОСТ Р 51583-2014 c) ГОСТ Р ИСО/МЭК ТО 13335-5-2006 d) ГОСТ Р 56115-2014	ОПК-11, ОПК - 14, ОПК -7.2
4.	a	На каком этапе создания СЗИ АСЗИ осуществляется разработка модели угроз? a) формирование требований к системе защиты информации АСЗИ b) разработка(проектирование) системы защиты информации АСЗИ c) внедрение системы защиты информации АСЗИ d) аттестация АСЗИ по требованиям безопасности информации и ввод в действие	ОПК-11, ОПК - 14, ОПК -7.2
5.	b	На каком этапе создания СЗИ АСЗИ осуществляется разработка эксплуатационной документации на СЗИ? a) формирование требований к системе защиты информации АСЗИ	ОПК-11, ОПК -

		b) разработка(проектирование) системы защиты информации АСЗИ c) внедрение системы защиты информации АСЗИ d) аттестация АСЗИ по требованиям безопасности информации и ввод в действие	14, ОПК -7.2
6.	b	На каком этапе создания СЗИ АСЗИ определяются типы субъектов доступа и объектов доступа, являющихся объектами защиты? a) формирование требований к системе защиты информации АСЗИ b) разработка(проектирование) системы защиты информации АСЗИ c) внедрение системы защиты информации АСЗИ d) аттестация АСЗИ по требованиям безопасности информации и ввод в действие	ОПК-11, ОПК - 14, ОПК -7.2
7.	b	На каком этапе создания СЗИ АСЗИ выбираются меры защиты информации, подлежащие реализации в системе защиты информации информационной системы? a) формирование требований к системе защиты информации АСЗИ b) разработка(проектирование) системы защиты информации АСЗИ c) внедрение системы защиты информации АСЗИ d) аттестация АСЗИ по требованиям безопасности информации и ввод в действие	ОПК-11, ОПК - 14, ОПК -7.2
8.	b	На каком этапе создания СЗИ АСЗИ осуществляется макетирование и тестирование СЗИ ИС? a) формирование требований к системе защиты информации АСЗИ b) разработка(проектирование) системы защиты информации АСЗИ c) внедрение системы защиты информации АСЗИ d) аттестация АСЗИ по требованиям безопасности информации и ввод в действие	ОПК-11, ОПК - 14, ОПК -7.2
9.	c	На каком этапе создания СЗИ АСЗИ осуществляется установка и настройка средств защиты информации? a) формирование требований к системе защиты информации АСЗИ b) разработка(проектирование) системы защиты информации АСЗИ c) внедрение системы защиты информации АСЗИ d) аттестация АСЗИ по требованиям безопасности информации и ввод в действие	ОПК-11, ОПК - 14, ОПК -7.2

10.	c	На каком этапе создания СЗИ АСЗИ осуществляется внедрение организационных мер защиты? a) формирование требований к системе защиты информации АСЗИ b) разработка(проектирование) системы защиты информации АСЗИ c) внедрение системы защиты информации АСЗИ d) аттестация АСЗИ по требованиям безопасности информации и ввод в действие	ОПК-11, ОПК - 14, ОПК -7.2
11.	c	На каком этапе создания СЗИ АСЗИ осуществляются приемочные испытания системы защиты информации? a. формирование требований к системе защиты информации АСЗИ a) разработка(проектирование) системы защиты информации АСЗИ b) внедрение системы защиты информации АСЗИ c) аттестация АСЗИ по требованиям безопасности информации и ввод в действие	ОПК-11, ОПК - 14, ОПК -7.2
12.	b	Выберите верное утверждение a) аттестация объекта информатизации проводится после начала обработки информации, подлежащей защите b) аттестация объекта информатизации проводится до начала обработки информации, подлежащей защите	ОПК-11, ОПК - 14, ОПК -7.2
13.	a	Как часто рекомендуется проводить контроль состояния системы защиты информации? a) не реже 1 раза в год b) не реже 1 раза в месяц c) не реже 1 раза в три года d) не реже 1 раза в пять лет	ОПК-11, ОПК - 14, ОПК -7.2
14.	a	На какой стадии создания СЗИ АСЗИ определяется перечень информации о АСЗИ, подлежащей защите? a) формирование требований к системе защиты информации АСЗИ b) разработка(проектирование) системы защиты информации АСЗИ c) внедрение системы защиты информации АСЗИ d) аттестация АСЗИ по требованиям безопасности информации и ввод в действие	ОПК-11, ОПК - 14, ОПК -7.2

15.	a	На каком этапе создания СЗИ АСЗИ осуществляется классификация информационной системы? a) формирование требований к системе защиты информации АСЗИ b) разработка(проектирование) системы защиты информации АСЗИ c) внедрение системы защиты информации АСЗИ d) аттестация АСЗИ по требованиям безопасности информации и ввод в действие	ОПК-11, ОПК - 14, ОПК -7.2
16.	a	На каком этапе создания СЗИ АСЗИ осуществляется классификация информационной системы? a) формирование требований к системе защиты информации АСЗИ b) разработка(проектирование) системы защиты информации АСЗИ c) внедрение системы защиты информации АСЗИ d) аттестация АСЗИ по требованиям безопасности информации и ввод в действие	ОПК-11, ОПК - 14, ОПК -7.2
17.	a	На каком этапе создания СЗИ АСЗИ осуществляется разработка модели злоумышленника? a) формирование требований к системе защиты информации АСЗИ b) разработка(проектирование) системы защиты информации АСЗИ c) внедрение системы защиты информации АСЗИ d) аттестация АСЗИ по требованиям безопасности информации и ввод в действие	ОПК-11, ОПК - 14, ОПК -7.2
18.	Основные компоненты парольной системы включают: Интерфейс администрато Хранимая копия пароля. Базу данных учётных записей Все варианты	Какие основные компоненты включает в себя парольная система в автоматизированны х системах в защищённом исполнении?	

	верны.		
19.	Валидация — это процесс подтверждения фактов, что установленные требования выполняются для конкретного применения рабочего программного продукта.	Что такое валидация в контексте разработки автоматизированных систем?	
20.	Ключевые этапы включают: Формирование стратегии идентификации. Установление стандартов. Определение содержания и целей документации. Разработку и сопровождение документов.	Какие ключевые этапы включает процесс менеджмента программной документации в соответствии с ГОСТ Р ИСО/МЭК 12207—2010?	

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала (контрольных точек), оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

3. Критерии оценивания компетенций

Оценка «**отлично**» выставляется студенту, если он: предоставляет детальный отчет в котором демонстрирует умение применять основные принципы организации технического, программного обеспечения защищенных информационных систем; основные принципы оптимального проектирования защищенных информационных систем и основные принципы оценки показателей эффективности защищенных информационных систем; предоставляет детальный отчет с полным пояснением в котором демонстрирует способность осуществлять разработку проектных решений систем защиты, оформлять проектную документацию; использовать методы оптимального проектирования защищенных информационных и телекоммуникационных систем, а так же проводить методы оценки эффективности, надежности, отказоустойчивости и производительности решений по обеспечению защищенности информационных и телекоммуникационных систем; предоставляет детальный отчет, в котором демонстрирует способность осуществлять разработку, внедрение и эксплуатацию автоматизированных систем в защищенном исполнении с учетом требований по защите информации; предоставляет детальный отчёт с обоснованием необходимости создания автоматизированных систем в защищенном исполнении; предоставляет детальный отчёт по формированию требований к автоматизированным системам в защищенном исполнении; предоставляет детальный отчет с демонстрацией способности осуществлять администрирование и контроль функционирования автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации; предоставляет детальный отчет, где демонстрирует способность осуществлять разработку проектных и организационных решений; предоставляет детальный отчет, где демонстрирует способность формировать требования к автоматизированным системам в защищенном исполнении; предоставляет детальный отчет, где демонстрирует способность осуществлять администрирование и контроль функционирования автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации.

Оценка «**хорошо**» выставляется студенту в случае, когда он предоставляет отчет в котором демонстрирует умение применять основные принципы организации технического, программного обеспечения защищенных информационных систем; основные принципы оптимального проектирования защищенных информационных систем и основные принципы оценки показателей эффективности защищенных информационных систем; предоставляет отчет с пояснением в котором демонстрирует способность осуществлять разработку проектных решений систем защиты, оформлять проектную документацию; использовать методы оптимального проектирования защищенных информационных и телекоммуникационных систем, а так же проводить методы оценки эффективности, надежности, отказоустойчивости и производительности решений по обеспечению защищенности информационных и телекоммуникационных систем; предоставляет отчет, в котором демонстрирует способность осуществлять разработку, внедрение и эксплуатацию автоматизированных систем в защищенном исполнении с учетом требований по защите информации; предоставляет отчёт с обоснованием необходимости создания

автоматизированных систем в защищенном исполнении; предоставляет отчёт по формированию требований к автоматизированным системам в защищенном исполнении; предоставляет отчет с демонстрацией способности осуществлять администрирование и контроль функционирования автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации; предоставляет отчет, где демонстрирует способность осуществлять разработку проектных и организационных решений; предоставляет отчет, где демонстрирует способность формировать требования к автоматизированным системам в защищенном исполнении; предоставляет отчет, где демонстрирует способность осуществлять администрирование и контроль функционирования автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации.

Оценка «**удовлетворительно**» выставляется студенту, если он предоставляет неполный отчет в котором демонстрирует умение применять основные принципы организации технического, программного обеспечения защищенных информационных систем; основные принципы оптимального проектирования защищенных информационных систем и основные принципы оценки показателей эффективности защищенных информационных систем; предоставляет неполный отчет с неполным пояснением в котором демонстрирует способность осуществлять разработку проектных решений систем защиты, оформлять проектную документацию; использовать методы оптимального проектирования защищенных информационных и телекоммуникационных систем, а так же проводить методы оценки эффективности, надежности, отказоустойчивости и производительности решений по обеспечению защищенности информационных и телекоммуникационных систем; предоставляет неполный отчет, в котором демонстрирует способность осуществлять разработку, внедрение и эксплуатацию автоматизированных систем в защищенном исполнении с учетом требований по защите информации; предоставляет неполный отчёт с обоснованием необходимости создания автоматизированных систем в защищенном исполнении; предоставляет неполный отчёт по формированию требований к автоматизированным системам в защищенном исполнении; предоставляет неполный отчет с демонстрацией способности осуществлять администрирование и контроль функционирования автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации; предоставляет неполный отчет, где демонстрирует способность осуществлять разработку проектных и организационных решений; предоставляет неполный отчет, где демонстрирует способность формировать требования к автоматизированным системам в защищенном исполнении; предоставляет неполный отчет, где демонстрирует способность осуществлять администрирование и контроль функционирования автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации.

Оценка «**неудовлетворительно**» выставляется, если студент: не предоставляет отчет в котором демонстрирует умение применять основные принципы организации технического, программного обеспечения защищенных информационных систем; основные принципы оптимального проектирования защищенных информационных систем и основные принципы оценки показателей эффективности защищенных информационных систем; не предоставляет отчет в котором демонстрирует способность осуществлять разработку проектных решений систем защиты, оформлять проектную документацию; использовать методы оптимального проектирования защищенных информационных и телекоммуникационных систем, а так же проводить методы оценки эффективности, надежности, отказоустойчивости и производительности решений по обеспечению защищенности информационных и телекоммуникационных систем; не предоставляет отчет, в котором демонстрирует способность осуществлять разработку, внедрение и эксплуатацию автоматизированных систем в защищенном исполнении с учетом требований по защите информации; не предоставляет отчёт с обоснованием необходимости

создания автоматизированных систем в защищенном исполнении; не предоставляет отчёт по формированию требований к автоматизированным системам в защищенном исполнении; не предоставляет отчет с демонстрацией способности осуществлять администрирование и контроль функционирования автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации; не предоставляет отчет, где демонстрирует способность осуществлять разработку проектных и организационных решений; не предоставляет отчет, где демонстрирует способность формировать требования к автоматизированным системам в защищенном исполнении; не предоставляет отчет, где демонстрирует способность осуществлять администрирование и контроль функционирования автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации.