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
Т.А. Гробова
Ф.И.О.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Защищенные информационные системы
название дисциплины (модуля)

Направление подготовки	10.04.01 «Информационная безопасность»
Направленность (профиль)	Информационная безопасность киберфизических систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	2,3

Введение

1. Назначение: проведение текущего контроля успеваемости и промежуточной аттестации по дисциплине «Защищенные информационные системы».

2. ФОС является приложением к программе дисциплины «Защищенные информационные системы» в соответствии с образовательной программой по направлению подготовки 10.04.01 Информационная безопасность (профиль «Информационная безопасность киберфизических систем») по дисциплине «Защищенные информационные системы»

3. Разработчик Орёл Д.В., доцент кафедры

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель: Петренко В. И., заведующий кафедрой

Члены экспертной группы: Минкина Т. В., доцент кафедры

Рачков В. Е., доцент кафедры

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

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.04.01 Информационная безопасность (профиль «Информационная безопасность киберфизических систем») и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Защищенные информационные системы».

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 компетенции(й),			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание				
ИД-1 ОПК-1 проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности	Не умеет проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности	Плохо проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности	Хорошо проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности	Самостоятельно проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности
ИД-3 ОПК-1 разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	Не разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	Почти разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	Умеет разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	Сразу разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности
Компетенция: ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности				
ИД-2 ОПК-2 выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных	Не умеет выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных	Не выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей и	Умеет выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей и	Уверенно выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных

систем и сетей и систем обеспечения информационной безопасностью	систем и сетей и систем обеспечения информационной безопасностью	систем обеспечения информационной безопасностью	систем обеспечения информационной безопасностью	систем и сетей и систем обеспечения информационной безопасностью
ИД-3 ОПК-2 решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	Не решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	Не достаточно решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	Хорошо решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	С уверенностью решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью

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 ОФО семестр 2,3	
1.	A, B, C, D	Под автоматизированной системой обработки информации (АС) понимать совокупность следующих объектов: (выберите несколько вариантов) A. средств вычислительной техники B. программного обеспечения C. каналов связи D. информации на различных носителях E. пользователей F. администраторов G. средств негласного получения информации	ОПК-1
2.	A, B	Информационная безопасность АС рассматривается как состояние системы, при котором: (выберите несколько вариантов) A. Система способна противостоять дестабилизирующему воздействию внутренних и внешних угроз B. Функционирование и сам факт наличия системы не создают угроз для внешней среды и для элементов самой системы C. Система способна противостоять дестабилизирующему воздействию только внутренних угроз D. Функционирование системы не создают угроз для элементов самой системы	ОПК-1
3.	A, B, C	Информационная безопасность обычно рассматривается как совокупность следующих трёх базовых свойств защищаемой информации: A. конфиденциальность B. целостность C. доступность D. достоверность E. воспроизводимость F. логичность G. последовательность	ОПК-1

		H. объективность	
4.	A	Свойство конфиденциальности информации A. означает, что доступ к информации могут получить только легальные пользователи B. обеспечивает, что защищаемая информация может быть изменена только законными и имеющими соответствующие полномочия пользователями C. обеспечивает, что информация внутренне непротиворечива и (если данное свойство применимо) отражает реальное положение вещей D. гарантирует беспрепятственный доступ к защищаемой информации для законных пользователей	ОПК-1
5.	D	Свойство доступности информации A. означает, что доступ к информации могут получить только легальные пользователи B. обеспечивает, что защищаемая информация может быть изменена только законными и имеющими соответствующие полномочия пользователями C. обеспечивает, что информация внутренне непротиворечива и (если данное свойство применимо) отражает реальное положение вещей D. гарантирует беспрепятственный доступ к защищаемой информации для законных пользователей	ОПК-1
6.	B, C	Свойство целостности информации A. означает, что доступ к информации могут получить только легальные пользователи B. обеспечивает, что защищаемая информация может быть изменена только законными и имеющими соответствующие полномочия пользователями C. обеспечивает, что информация внутренне непротиворечива и (если данное свойство применимо) отражает реальное положение вещей D. гарантирует беспрепятственный доступ к защищаемой информации для законных пользователей	ОПК-1
7.	A, C, D	К угрозам, источником которых является человек, можно отнести: A. внедрение агентов в ряды персонала АС со стороны конкурирующей организации B. некомпетентное использование системных утилит C. продажа базы данных, обрабатываемой в АС D. хранение стикера с паролем на мониторе рабочего компьютера E. уязвимость в операционной системе F. внедрение в систему кейлоггеров	ОПК-1

		G. подключенный к сети личный ноутбук сотрудника	
8.	B, E	К угрозам, источником которых являются санкционированные программно¬аппаратные средства, можно отнести: A. внедрение агентов в ряды персонала АС со стороны конкурирующей организации B. некомпетентное использование системных утилит C. продажа базы данных, обрабатываемой в АС D. хранение стикера с паролем на мониторе рабочего компьютера E. уязвимость в операционной системе F. внедрение в систему кейлоггеров G. подключенный к сети личный ноутбук сотрудника	ОПК-1
9.	F, G	К угрозам, источником которых является несанкционированные программно¬аппаратные средства, можно отнести: A. внедрение агентов в ряды персонала АС со стороны конкурирующей организации B. некомпетентное использование системных утилит C. продажа базы данных, обрабатываемой в АС D. хранение стикера с паролем на мониторе рабочего компьютера E. уязвимость в операционной системе F. внедрение в систему кейлоггеров G. подключенный к сети личный ноутбук сотрудника	ОПК-1
10.	A, B, C, D	Всё множество использующих в настоящее время методов аутентификации можно разделить на 4 большие группы: A. Методы, основанные на знании некоторой секретной информации B. Методы, основанные на использовании уникального предмета C. Методы, основанные на использовании биометрических характеристик человека D. Методы, основанные на информации, ассоциированной с пользователем E. Методы, основанные на разделении секрета F. Методы, основанные на взаимном доверии G. Методы, основанные на нулевом уровне доверия (zero trust)	ОПК-1
11.	D, E, F	В качестве примера метода аутентификации, основанного на использовании уникального предмета,	ОПК-1

		может служить A. парольная защита B. пин-код C. секретное слово D. смарт-карта E. токен F. электронный ключ G. отпечаток пальца H. фотография I. голос J. GPS-координаты K. код из Google Authenticator L. время прохождения аутентификации	
12.	A, B, C	В качестве примера метода аутентификации, основанного на знании некоторой секретной информации, может служить A. парольная защита B. пин-код C. секретное слово D. смарт-карта E. токен F. электронный ключ G. отпечаток пальца H. фотография I. голос J. GPS-координаты K. код из Google Authenticator L. время прохождения аутентификации	ОПК-1
13.	G, H, I	В качестве примера метода аутентификации, основанного на использовании биометрических характеристик человека, может служить	ОПК-1

		A. парольная защита B. пин-код C. секретное слово D. смарт-карта E. токен F. электронный ключ G. отпечаток пальца H. фотография I. голос J. GPS-координаты K. код из Google Authenticator L. время прохождения аутентификации	
14.	J, K, L	В качестве примера метода аутентификации, основанного на информации, ассоциированной с пользователем, может служить A. парольная защита B. пин-код C. секретное слово D. смарт-карта E. токен F. электронный ключ G. отпечаток пальца H. фотография I. голос J. GPS-координаты K. код из Google Authenticator L. время прохождения аутентификации	ОПК-1
15.	A, B, C, D	Политика безопасности АС должна обязательно включать в себя следующие элементы (механизмы безопасности): A. произвольное управление доступом	ОПК-1

		B. безопасность повторного использования объектов C. метки безопасности D. принудительное управление доступом E. метрика ресурсов F. выборочное управление потоками	
16.	A, E, F	Так называется метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту A. произвольное управление доступом B. хаотический доступ C. делегирующее управление D. доступ без авторизации E. Произвольный доступ F. Произвольное управление	ОПК-1
17.	A	Это важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из "мусора". Безопасность должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом. A. Безопасность повторного использования объектов B. «Нет чтения вверх» C. «Нет записи вниз»	ОПК-1
18.	A	Это состоят из двух частей - уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество, категории - неупорядоченное. Назначение последних - описать предметную область, к которой относятся данные. A. метки безопасности B. метки времени C. лог-файлы	ОПК-1
19.	A	Для реализации этого управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта описывает его благонадежность, метка объекта - степень	ОПК-1

		конфиденциальности содержащейся в нем информации. A. принудительного B. произвольного C. хаотичного	
20.	A	Идентификация – это A. присвоение субъектам доступа уникальных идентификаторов и сравнение таких идентификаторов с перечнем возможных B. проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности	ОПК-1
21.	B	Аутентификация – это A. присвоение субъектам доступа уникальных идентификаторов и сравнение таких идентификаторов с перечнем возможных B. проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности	ОПК-1
22.	A	Оценочные стандарты в области информационной безопасности A. направлены на классификацию информационных систем и средств защиты по требованиям безопасности B. регламентируют различные аспекты реализации средств защиты	ОПК-1
23.	B	Технические спецификации в области информационной безопасности A. направлены на классификацию информационных систем и средств защиты по требованиям безопасности B. регламентируют различные аспекты реализации средств защиты	ОПК-2
24.	A	Система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа – это A. доверенная система B. многоуровневая система C. высокоранговая система	ОПК-2
25.	A, B	Степень доверия к автоматизированной системе оценивается по двум основным критериям:	ОПК-2

		A. Политика безопасности B. Уровень гарантированности C. Степень надёжности D. Уровень секретности	
26.	A	Это - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть и она. В зависимости от сформулированной её можно выбирать конкретные механизмы обеспечения безопасности. A. политика информационной безопасности B. Конституция Российской Федерации C. нормативная база в области информационной безопасности	ОПК-1
27.	A	Это - мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Это показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. A. уровень гарантированности B. степень свободы C. величина достоверности	ОПК-1
28.	A, B	Из пассивных аспектов защиты в «Оранжевой книге» рассматривается два вида гарантированности: A. операционная B. технологическая C. функциональная D. структурная E. логическая	ОПК-1
29.	F	Операционная гарантированность не включает в себя проверку следующего элемента: A. архитектура системы B. целостность системы C. проверка тайных каналов передачи информации	ОПК-1

		D. доверенное администрирование E. доверенное восстановление после сбоев F. многократное резервирование	
30.	A	Какова точная формулировка функции монитора обращений? A. контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями) B. проведение в жизнь политики безопасности C. обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа	ОПК-1
31.	A, B, C	Монитор обращений должен обладать тремя качествами: A. Изолированность B. Полнота C. Верифицируемость D. Доступность E. Зарезервированность	ОПК-1
32.		Перечислите функции и методы изучения информационных систем. Раскройте содержание понятия информационных систем	ОПК-1
33.		Перечислите виды информационных систем	ОПК-2
34.		Перечислите основные угрозы безопасности. Назовите стадии развития угрозы и меры по ее устранению.	ОПК-2
35.		Опишите основные этапы устранения угрозы безопасности в информационных системах	ОПК-2
36.		Перечислите основной анализ требований и стандартов. Раскройте понятие защищенной информационной системы.	ОПК-2
37.		Для чего необходимо осуществлять анализ требований стандартов информационной безопасности?	ОПК-2
38.		Раскройте понятие «Модель безопасности». Раскройте понятие «Политика безопасности»	ОПК-2
39.		Назовите основные принципы работы политики безопасности	ОПК-2

40.		Опишите процесс межсетевого экранирования. Раскройте понятие межсетевого экранирования	ОПК-2
41.		Раскройте понятие «виртуальные защищенные сети». Для чего необходим VPN	ОПК-2

2. Описание шкалы оценивания

Оценка «отлично» выставляется обучающемуся, если студент продемонстрировал высокое умение применять полученные знания на практике через решение конкретного задания, свободно без затруднений справился с поставленным заданием, показав владение разносторонними приемами и навыками его выполнения, не допустил ошибок и неточностей.

Оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал умение применять полученные знания на практике через решение конкретного задания, справился с поставленным заданием, показав владение необходимыми приемами и навыками его выполнения, при этом допустил незначительную ошибку.

Оценка «удовлетворительно» выставляется обучающемуся, если студентпродемонстрировал посредственное умение применять полученные знания на практике, с трудом справился с поставленным заданием, при этом допустил значительную ошибку.

Оценка «неудовлетворительно» выставляется обучающемуся, если студент не продемонстрировал умение применять полученные знания на практике через решение конкретного задания, не справился с поставленнымзаданием или допустил при его решении серьезную ошибку.

Процедура проведения данного оценочного мероприятия включает в себя Предлагаемые студенту задания позволяют проверить ОПК-1, ОПК-2 компетенции.

Для подготовки к данному оценочному мероприятию необходимо ответить на вопросы, предлагаемые преподавателем, ведущим дисциплину «Защищенные информационные системы» Знания оцениваются преподавателем согласно правильно отвеченными вопросами.

Рейтинговая система оценки не предусмотрено для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной формы обучения.

3. Критерии оценивания компетенций*

Оценка «отлично» выставляется, если студент продемонстрировал высокое владение самостоятельно проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности; разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивать эффективность решений и анализирует показатели деятельности; уверенно выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью; с уверенностью решать типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью.

Оценка «хорошо» выставляется, если студент продемонстрировал умение проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности; разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивать эффективность решений и анализирует показатели деятельности; выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью; решать типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью.

Оценка «удовлетворительно» выставляется, если студент продемонстрировал посредственное умение проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности; разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, не всегда оценивает эффективность решений и не достаточно анализирует показатели деятельности; не уверенно выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью; с посредственно решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной

безопасностью.

Оценка «неудовлетворительно» выставляется, если студент не продемонстрировал умение проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности; не разрабатывает и не обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, не оценивает эффективность решений и не анализирует показатели деятельности; не решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью.