

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Антоновна

Должность: и.о. декана факультета математики и компьютерных наук имени
профессора Н.И. Червякова

Дата подписания: 22.09.2026 11:01:35

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
Грובה Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
Технологии обеспечения информационной безопасности

Направление подготовки	<u>10.04.01 Информационная безопасность</u>
Направленность (профиль)	<u>Математическое и программное обеспечение защиты информации</u>
Год начала обучения	<u>2026</u>
Форма обучения	<u>очная</u>
Реализуется в семестре	<u>1</u>

Ставрополь, 2026 г.

Введение

1. Назначение: проведение текущего контроля успеваемости и промежуточной аттестации по дисциплине «Технологии обеспечения информационной безопасности».

2. ФОС является приложением к программе дисциплины «Технологии обеспечения информационной безопасности» в соответствии с образовательной программой по направлению подготовки 10.04.01 Информационная безопасность (направленность (профиль) «Математическое и программное обеспечение защиты информации») по дисциплине «Технологии обеспечения информационной безопасности».

3. Разработчик: Петренко В.И., канд. техн. наук, доцент, заведующий кафедрой организации и технологии защиты информации.

4. Проведена экспертиза ФОС.

Члены экспертизы ФОС:

Председатель: Петренко В.И. – заведующий кафедрой;

Члены комиссии: Мандрица И.В., профессор кафедры;

Рачков В.Е., доцент кафедры;

Жук А.П., профессор 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 (направленность (профиль) «Математическое и программное обеспечение защиты информации») и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Технологии обеспечения информационной безопасности».

5. Срок действия ФОС: на срок реализации образовательной программы.

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

Компетенция (ии), индикатор (ы)	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 проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности	Проектирует информационные системы с учетом отдельных технологий обеспечения информационной безопасности, допуская существенные ошибки	Проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности, допуская отдельные неточности	Самостоятельно и без ошибок проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности
ИД-2 ОПК-1 формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности	Не формирует актуальную модель угроз для автоматизированных информационных систем и не учитывает её положения при формировании требований технического задания	Формирует актуальную модель угроз не в полном объеме, учитывает её положения при формировании требований технического задания с существенными ошибками	Формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания, допуская отдельные неточности	Самостоятельно формирует актуальную модель угроз для автоматизированных информационных систем и в полном объеме учитывает её положения при формировании требований технического задания
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 не обосновывает критерии оценки эффективности проектируемой системы, не оценивает эффективность решений	Разрабатывает критерии оценки эффективности проектируемой системы, но не обосновывает их, недостаточно оценивает эффективность решений	Разрабатывает и обосновывает критерии оценки эффективности проектируемой системы, оценивает эффективность решений и анализирует показатели деятельности с отдельными неточностями	Самостоятельно разрабатывает и обосновывает критерии оценки эффективности проектируемой системы, оценивает эффективность решений и анализирует показатели деятельности
Компетенция: ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности				
ИД-1 ОПК-2 использует методы концептуального проектирования технологий обеспечения информационной безопасности	Не использует методы концептуального проектирования технологий обеспечения информационной безопасности	Использует отдельные методы концептуального проектирования технологий обеспечения информационной безопасности, допуская существенные ошибки	Использует методы концептуального проектирования технологий обеспечения информационной безопасности, допуская отдельные неточности	Уверенно и самостоятельно использует методы концептуального проектирования технологий обеспечения информационной безопасности
ИД-2 ОПК-2 выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	Не выбирает и не обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей	Выбирает методы решения задач для защиты информации компьютерных систем и сетей, но не обосновывает их преимущества	Выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей, допуская отдельные неточности	Самостоятельно выбирает и полно обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью
Компетенция: ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи				

Компетенция (ии), индикатор (ы)	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
ИД-1 ОПК-5 применяет методы научных исследований в научной деятельности, в частности, при написании магистерской диссертации и научных статей	Не применяет методы научных исследований в научной деятельности	Применяет отдельные методы научных исследований только под руководством преподавателя (научного руководителя)	Применяет методы научных исследований в научной деятельности, допуская отдельные неточности в выборе метода и обработке результатов	Самостоятельно и обоснованно применяет методы научных исследований, в том числе при написании магистерской диссертации и научных статей
ИД-2 ОПК-5 оформляет научно-технические отчеты и обзоры по результатам проведенных экспериментальных исследований	Не оформляет научно- технические отчеты и обзоры по результатам проведенных экспериментальных исследований	Оформляет научно- технические отчеты и обзоры с нарушением установленных требований к их структуре и содержанию	Оформляет научно- технические отчеты и обзоры по результатам проведенных экспериментальных исследований, допуская отдельные отступления от установленных требований	Самостоятельно оформляет научно- технические отчеты и обзоры в полном соответствии с установленными требованиями

2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Форма обучения – очная, семестр 1

Номер задания	Правильный ответ	Содержание вопроса	Компетенция, индикатор
1	А	Сведения (сообщения, данные) независимо от формы их представления: А. Информация В. Информационные технологии С. Информационная система D. Информационно-телекоммуникационная сеть Е. Обладатель информации	ИД-1 ОПК-1
2	В	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов: А. Информация В. Информационные технологии С. Информационная система D. Информационно-телекоммуникационная сеть Е. Обладатель информации	ИД-1 ОПК-1
3	D	Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники, это: А. База данных В. Информационная технология С. Информационная система D. Информационно-телекоммуникационная сеть	ИД-1 ОПК-1
4	Е	Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации: А. Источник информации В. Потребитель информации С. Уничтожитель информации D. Носитель информации Е. Обладатель информации	ИД-1 ОПК-1
5	А	Информация, переданная или полученная пользователем информационно-телекоммуникационной сети: А. Электронное сообщение В. Информационное сообщение С. Текстовое сообщение D. Визуальное сообщение Е. SMS-сообщение	ИД-1 ОПК-1
6	А	Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные, это: А. Информационная система персональных данных В. База данных С. Централизованное хранилище данных D. Сервер	ИД-1 ОПК-1
7	D	Действия с персональными данными (согласно закону), включая сбор, систематизацию, накопление, хранение, использование, распространение и т. д., это: А. «Исправление персональных данных» В. «Работа с персональными данными» С. «Преобразование персональных данных» D. «Обработка персональных данных» Е. «Изменение персональных данных»	ИД-1 ОПК-1
8	А	Согласно рекомендациям Х.800 аутентификация может быть реализована на: А. сетевом уровне В. транспортном уровне	ИД-2 ОПК-2

Номер задания	Правильный ответ	Содержание вопроса	Компетенция, индикатор
		С. прикладном уровне	
9	А, В	В число целей политики безопасности верхнего уровня входят: А. решение сформировать или пересмотреть комплексную программу безопасности В. обеспечение базы для соблюдения законов и правил С. обеспечение конфиденциальности почтовых сообщений	ИД-3 ОПК-1
10	С	Для безопасной передачи данных по каналам сети Интернет используется технология: А. WWW В. DICOM С. VPN D. FTP E. XML	ИД-2 ОПК-2
11	С	Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа: А. Антивирус В. Замок С. Брандмауэр D. Криптография E. Экспертная система	ИД-2 ОПК-2
12	А	Несанкционированный доступ к информации – это: А. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально В. Работа на чужом компьютере без разрешения его владельца С. Вход на компьютер с использованием данных другого пользователя D. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей E. Доступ к СУБД под запрещенным именем пользователя	ИД-2 ОПК-1
13	А	«Персональные данные» – это: А. Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу В. Фамилия, имя, отчество физического лица С. Год, месяц, дата и место рождения, адрес физического лица D. Адрес проживания физического лица E. Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»	ИД-1 ОПК-1
14	Е	В данном случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности: А. Выход в Интернет без разрешения администратора В. При установке компьютерных игр С. В случаях установки нелицензионного ПО D. В случае невыхода из информационной системы E. В любом случае неправомерного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности	ИД-1 ОПК-1
15	С	Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия: А. Нет, только к административной ответственности В. Нет, если это государственное предприятие С. Да	ИД-1 ОПК-1

Номер задания	Правильный ответ	Содержание вопроса	Компетенция, индикатор
		Д. Да, но только в случае, если действия сотрудника нанесли непоправимый вред Е. Да, но только в случае осознанных неправомерных действий сотрудника	
16	А	Выберите, можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере: А. Нет, ни при каких обстоятельствах В. Нет, но для отправки срочных и особо важных писем можно С. Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера Д. Можно, если информацию предварительно заархивировать с паролем Е. Можно, если других способов электронной передачи данных в настоящий момент нет, а информацию нужно переслать срочно	ИД-2 ОПК-1
17	С	Для того чтобы снизить вероятность утраты информации, необходимо: А. Регулярно производить антивирусную проверку компьютера В. Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок С. Регулярно копировать информацию на внешние носители Д. Защитить вход на компьютер к данным паролем Е. Проводить периодическое обслуживание ПК	ИД-2 ОПК-1
18	А	Пароль пользователя должен: А. Содержать цифры и буквы, знаки препинания и быть сложным для угадывания В. Содержать только цифры С. Содержать только буквы Д. Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т. п.) Е. Быть простым и легко запоминаться	ИД-2 ОПК-2
19	Е	Доступ к информации – это: А. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя В. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц С. Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц Д. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети Е. Возможность получения информации и ее использования	ИД-1 ОПК-1
20	А	Документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, это: А. Конфиденциальная информация В. Документы оферты и договоров С. Факс Д. Личный дневник Е. Законы РФ	ИД-1 ОПК-1
21	А, В	Самыми опасными источниками внутренних угроз являются: А. некомпетентные руководители В. обиженные сотрудники С. любопытные администраторы	ИД-2 ОПК-1

Номер задания	Правильный ответ	Содержание вопроса	Компетенция, индикатор
22	С	Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности: А. просчеты при администрировании информационных систем В. необходимость постоянной модификации информационных систем С. сложность современных информационных систем	ИД-2 ОПК-1
23	В	Для внедрения логических бомб чаще всего используются ошибки типа: А. отсутствие проверок кодов возврата В. переполнение буфера С. нарушение целостности транзакций	ИД-2 ОПК-1
24	В	Окно опасности появляется, когда: А. становится известно о средствах использования уязвимости В. появляется возможность использовать уязвимость С. реализована угроза	ИД-2 ОПК-1
25	А, С	Уголовный кодекс РФ предусматривает наказания за: А. создание, использование и распространение вредоносных программ В. ведение личной корреспонденции на производственной технической базе С. нарушение правил эксплуатации информационных систем	ИД-1 ОПК-1
26	В	Под определение средств защиты информации, данное в Законе «О государственной тайне», подпадают: А. средства выявления злоумышленной активности В. средства обеспечения отказоустойчивости С. средства контроля эффективности защиты информации	ИД-3 ОПК-1
27	А, В	Уровень безопасности В согласно «Оранжевой книге» характеризуется: А. произвольным управлением доступом В. принудительным управлением доступом С. верифицируемой безопасностью	ИД-1 ОПК-2
28	А, С	В число классов требований доверия безопасности «Общих критериев» входят: А. разработка В. оценка профиля защиты С. сертификация	ИД-3 ОПК-1
29	В	Согласно «Оранжевой книге» политика безопасности включает в себя следующие элементы: А. периметр безопасности В. метки безопасности С. сертификаты безопасности	ИД-1 ОПК-2
30	В	Согласно рекомендациям Х.800 выделяются следующие сервисы безопасности: А. управление квотами В. управление доступом С. экранирование	ИД-1 ОПК-2
31	С	Уровень безопасности А согласно «Оранжевой книге» характеризуется: А. произвольным управлением доступом В. принудительным управлением доступом С. верифицируемой безопасностью	ИД-1 ОПК-2
32	–	Информация – фактор существования и развития общества.	ИД-1 ОПК-1
33	–	Нормы права, правоотношения, субъекты и объекты права, юридические факты. Источники права.	ИД-1 ОПК-1
34	–	Термины и определения в области защиты информации.	ИД-1 ОПК-1
35	–	Международная нормативная база обеспечения безопасности.	ИД-3 ОПК-1
36	–	Правовые основы использования персональных данных.	ИД-1 ОПК-1

Номер задания	Правильный ответ	Содержание вопроса	Компетенция, индикатор
37	–	Понятие информационной безопасности. Основные составляющие.	ИД-1 ОПК-1
38	–	Средства антивирусной защиты.	ИД-2 ОПК-2
39	–	Идентификация и аутентификация пользователей. Парольная аутентификация. Система S/KEY.	ИД-2 ОПК-2
40	–	VPN сетевого уровня. Протокол IPsec.	ИД-2 ОПК-2
41	–	Методы научных исследований: классификация теоретических и эмпирических методов, область их применения при решении задач обеспечения информационной безопасности.	ИД-1 ОПК-5
42	–	Планирование экспериментального исследования защищенности информационной системы: постановка задачи, выбор показателей, условия проведения эксперимента.	ИД-1 ОПК-5
43	–	Обработка и интерпретация результатов экспериментальных исследований в области защиты информации, оценка достоверности полученных результатов.	ИД-1 ОПК-5
44	–	Постановка задачи научного исследования по теме магистерской диссертации в области обеспечения информационной безопасности.	ИД-1 ОПК-5
45	–	Структура и правила оформления научно-технического отчета о результатах проведенного исследования.	ИД-2 ОПК-5
46	–	Требования к оформлению обзора источников и библиографического списка (ГОСТ Р 7.0.100-2018).	ИД-2 ОПК-5
47	–	Подготовка научной статьи по результатам исследования: структура, аннотация, ключевые слова, выводы.	ИД-2 ОПК-5
48	–	Подготовка и представление научного доклада по результатам выполненного исследования.	ИД-2 ОПК-5

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 не более одной ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если студент продемонстрировал посредственное умение применять полученные знания на практике через решение конкретного задания, с трудом справился с поставленным заданием, при этом допустил не более двух ошибок.

Оценка «неудовлетворительно» выставляется обучающемуся, если студент не продемонстрировал умение применять полученные знания на практике через решение конкретного задания, не справился с поставленным заданием или допустил при его решении три и более серьезные ошибки.

Рейтинговая система оценки не предусмотрена для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, а также для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной форм обучения.

3. Критерии оценивания компетенций

Оценка «отлично» выставляется, если студент самостоятельно проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности; формирует актуальную модель угроз для автоматизированных

информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности; самостоятельно разрабатывает и обосновывает критерии оценки эффективности проектируемой системы, оценивает эффективность решений и анализирует показатели деятельности; уверенно использует методы концептуального проектирования технологий обеспечения информационной безопасности; самостоятельно выбирает и полно обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей; обоснованно применяет методы научных исследований и оформляет научно-технические отчеты и обзоры в полном соответствии с установленными требованиями.

Оценка «хорошо» выставляется, если студент проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности, допуская отдельные неточности; формирует актуальную модель угроз и учитывает её положения при формировании требований технического задания; разрабатывает критерии оценки эффективности проектируемой системы, оценивает эффективность решений и анализирует показатели деятельности; использует методы концептуального проектирования технологий обеспечения информационной безопасности; выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей; применяет методы научных исследований и оформляет научно-технические отчеты и обзоры с отдельными отступлениями от установленных требований.

Оценка «удовлетворительно» выставляется, если студент проектирует информационные системы с учетом отдельных технологий обеспечения информационной безопасности, допуская существенные ошибки; посредственно формирует актуальную модель угроз и учитывает её положения при формировании требований технического задания; в основном разрабатывает критерии оценки эффективности проектируемой системы, недостаточно оценивает эффективность решений; использует не все методы концептуального проектирования технологий обеспечения информационной безопасности; выбирает методы решения задач защиты информации, но не обосновывает их преимущества; применяет отдельные методы научных исследований только под руководством преподавателя, оформляет научно-технические отчеты и обзоры с нарушением установленных требований.

Оценка «неудовлетворительно» выставляется, если студент не проектирует информационные системы с учетом технологий обеспечения информационной безопасности; не формирует актуальную модель угроз и не учитывает её положения при формировании требований технического задания; не разрабатывает критерии оценки эффективности проектируемой системы; не использует методы концептуального проектирования технологий обеспечения информационной безопасности; не выбирает и не обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей; не применяет методы научных исследований и не оформляет научно-технические отчеты и обзоры.