Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ефанов Алексей Валерьевич
Должность: Директор Невинномысского технологического института (филиал) СКФУ
Дата подписания: 19.06.2026 17:58:20
Уникальный программный ключ:
49214306dd433e7a1b0f8632f645f9d53c99e3d0

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Директор НТИ (филиал) СКФУ
канд. техн. наук, доцент Ефанов А.В.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Информационная безопасность

Направление подготовки/специальность	09.03.02 Информационные системы и технологии
Направленность (профиль)/специализация	Информационные системы управления технологическими и сервисными процессами
Год начала обучения	2026
Форма обучения	очная заочная очно-заочная
Реализуется в семестре	8

Предисловие

1. Назначение: данный фонд оценочных средств предназначен для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине «Информационная безопасность».

2. ФОС является приложением к программе дисциплины «Информационная безопасность».

3. Разработчик: Кочеров Юрий Николаевич, доцент кафедры информационныхсистем, электропривода и автоматики, канд. техн. наук, доцент

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель: Кочеров Ю.Н., кандидат технических наук, доцент, доцент кафедры информационных систем, электропривода и автоматики

Члены комиссии:
Колдаев А.И., заведующий кафедрой информационных систем, электропривода и автоматики, кандидат технических наук, доцент
Евдокимов А.А., кандидат технических наук, доцент, доцент кафедры информационных систем, электропривода и автоматики

Представитель организации-работодателя:
Остапенко Н.А., кандидат технических наук, ведущий инженер-конструктор ООО «Корпоративный институт электротехнического приборостроения «Энергомера» филиала АО «Электротехнические заводы «Энергомера»

Экспертное заключение: ФОС рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Информационная безопасность».

5. Срок действия ФОС определяется сроком реализации образовательной программы.

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
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности				
Результаты обучения по дисциплине (модулю): Индикатор: ИД-2 ОПК-3 Обеспечивает защиту информации при решении стандартных профессиональных задач с использованием антивирусных средств, резервного копирования и соблюдения политик конфиденциальности. ИД-3 ОПК-3 Представляет результаты профессиональной деятельности с соблюдением требований библиографической культуры и норм информационной безопасности при оформлении отчетов и презентаций	Студент не знает базовых методов криптографической и антивирусной защиты. Не может запустить антивирус, не понимает сути резервного копирования. Демонстрирует полное игнорирование политик конфиденциальности или отсутствие навыков работы с соответствующим ПО. Студент не умеет оформлять отчеты по ГОСТу (список литературы составлен хаотично, структура отсутствует). При публикации материалов в открытых источниках оставляет персональные данные без защиты, демонстрируя полное отсутствие	Студент имеет общее представление о средствах защиты. Способен запустить антивирус или сделать резервную копию только по готовой инструкции (алгоритму). Не всегда понимает разницу между типами угроз и может нарушить политику конфиденциальности из-за непонимания последствий. Студент способен оформить отчет и список литературы, но с ошибками в оформлении по ГОСТу (не тот шрифт, ошибки в описании источников). Понимает необходимость защиты персональных данных, но на практике может забыть удалить конфиденциальную информацию из презентации перед публикацией.	Студент уверенно использует антивирусные программы и инструменты резервного копирования в стандартных ситуациях. Понимает важность политик конфиденциальности, соблюдает их, но при настройке защиты в нестандартных условиях может допускать незначительные технические ошибки или требовать подсказки. Студент правильно оформляет отчеты и списки литературы по ГОСТу. В основном соблюдает нормы информационной безопасности, но при публикации	Студент свободно и осознанно применяет методы криптографической и антивирусной защиты. Самостоятельно настраивает политики конфиденциальности и системы резервного копирования для корпоративных данных в локальных и облачных хранилищах, адаптируя их под специфику задачи. Способен не только использовать готовые средства, но и анализировать инциденты. Студент безупречно оформляет отчеты и

	навыков информационной безопасности.		может упустить из виду второстепенные детали (например, оставить данные автора в свойствах файла). Ошибки в оформлении незначительны и не системны.	презентации по ГОСТу, используя офисное ПО. При публикации в открытых источниках не только скрывает персональные данные, но и проверяет метаданные файлов, корректно anonymизирует информацию. Список литературы составлен идеально, с пониманием библиографической культуры.
ОПК-7 Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем				
Результаты обучения по дисциплине (модулю): Индикатор ИД-2 ОПК-7 Обосновывает выбор криптографических алгоритмов и программно-аппаратных средств реализации защиты информации при проектировании безопасных информационных систем.	Студент не ориентируется в криптографических алгоритмах. Не может назвать ни одного стандарта шифрования, не понимает разницы между шифрованием и хэшированием. Полностью отсутствует способность к анализу и выбору средств защиты для проектируемой системы.	Студент знает названия основных алгоритмов шифрования и хэширования. Может перечислить их отличия (симметричные/асимметричные), но затрудняется с обоснованным выбором под конкретную систему. Выбор делает интуитивно или по подсказке преподавателя, не проводя полноценного анализа требований.	Студент способен проанализировать требования и сравнить основные характеристики (скорость, длина ключа) популярных алгоритмов (ГОСТ, AES, RSA). Обосновывает выбор адекватного алгоритма, но сравнение ограничивается 2-3 параметрами, не углубляясь в тонкости реализации или потенциальные уязвимости.	Студент проводит глубокий сравнительный анализ алгоритмов шифрования и хэширования. Учитывает заданные ограничения (производительность, криптостойкость, среду реализации) и выбирает оптимальное решение. Способен математически обосновать, почему выбранный

				алгоритм лучше других в контексте конкретной задачи.

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 очная Семестр6, Форма обучения заочная семестр 8	
1.	получение «бесконечной» гаммы (ключевой последовательности), располагая относительно малой длиной самого секретного ключа	Какова цель использования генераторов псевдослучайных чисел при поточном шифровании? ~ формирование открытых ключей ~ защита информации от всех случайных или преднамеренных изменений ~ получение «бесконечной» гаммы (ключевой последовательности), располагая относительно малой длиной самого секретного ключа ~ защита информации от случайных помех при передаче и хранении сжатие информации	ОПК-3 ОПК-7
2.	количеством бит, которое может одновременно храниться в регистре сдвига	Чем определяется разрядность сдвигового регистра с обратной связью? ~ скоростью работы регистра ~ температурой окружающей среды ~ количеством входов в устройстве генерации функции обратной связи количеством бит, которое может одновременно храниться в регистре сдвига	ОПК-3 ОПК-7
3.	односторонней функцией	Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии ~ функцией Диффи-Хеллмана ~ односторонней функцией ~ функцией Эйлера криптографической функцией	ОПК-3 ОПК-7
4.	блочным алгоритмом симметричного шифрования	Алгоритм ГОСТ 28147-89 является ~ алгоритмом вычисления функции хеширования ~ блочным алгоритмом асимметричного шифрования ~ блочным алгоритмом симметричного шифрования алгоритмом формирования электронной цифровой подписи	ОПК-3 ОПК-7
5.	сообщение,	Что является особенностью использования режима CBC блочного шифра?	ОПК-3

	зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока	~ одинаковые сообщения при использовании разных векторов инициализации преобразуются в одинаковый шифротекст ~ сообщение, зашифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста в произвольном порядке ~ одинаковые блоки исходного текста преобразуются в одинаковый шифротекст ~ этот режим работает очень медленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока	ОПК-7
6.	10000010	Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0B5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид	ОПК-3 ОПК-7
7.	нет	Может ли шифр с конечным ключом быть совершенным? ~ да, если это алгоритм шифрования с открытым ключом ~ в зависимости от параметров шифра ~ нет ~ да	ОПК-3 ОПК-7
8.	в них для шифрования и расшифрования информации используется один и тот же ключ	Что общего имеют все методы шифрования с закрытым ключом? ~ в них для шифрования информации используется один ключ, а для расшифрования – другой ключ ~ в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов ~ в них для операций шифрования и расшифрования используется два разных ключа – открытый и закрытый в них для шифрования и расшифрования информации используется один и тот же ключ	ОПК-3 ОПК-7
9.	генерации псевдослучайных чисел	Для чего предназначен алгоритм Блюм-Блюма-Шуба (BBS)? ~ генерации псевдослучайных чисел	ОПК-3 ОПК-7

		~ для сжатия информации ~ для формирования открытых ключей для формирования хеш-кода	
10.	2, 5, 19, 37, 59, 101	Выберите вариант ответа, содержащий только простые числа ~ 2, 5, 19, 37, 59, 101 ~ 2, 7, 17, 37, 57, 107 ~ 2, 5, 19, 37, 59, 133 ~ 3, 7, 19, 39, 59, 10	ОПК-3 ОПК-7
11.	Разработка и конкретизация правовых нормативных актов обеспечения безопасности	К правовым методам, обеспечивающим информационную безопасность, относятся: ~ Разработка аппаратных средств обеспечения правовых данных ~ Разработка и установка во всех компьютерных правовых сетях журналов учета действий Разработка и конкретизация правовых нормативных актов обеспечения безопасности	ОПК-3 ОПК-7
12.	Перехват данных, хищение данных, изменение архитектуры системы	Основными источниками угроз информационной безопасности являются все указанное в списке: ~ Хищение жестких дисков, подключение к сети, инсайдерство ~ Перехват данных, хищение данных, изменение архитектуры системы Хищение данных, подкуп системных администраторов, нарушение регламента работы	ОПК-3 ОПК-7
13.	Персональная, корпоративная, государственная	**Виды информационной безопасности:** ~ Персональная, корпоративная, государственная ~ Клиентская, серверная, сетевая Локальная, глобальная, смешанная	ОПК-3 ОПК-7
14.		Цели информационной безопасности – своевременное обнаружение, предупреждение: ~ несанкционированного доступа, воздействия в сети ~ инсайдерства в организации чрезвычайных ситуаций	ОПК-3 ОПК-7
15.	Компьютерные сети, базы данных	Основные объекты информационной безопасности: ~ Компьютерные сети, базы данных	ОПК-3 ОПК-7

		Информационные системы, психологическое состояние пользователей Бизнес-ориентированные, коммерческие системы	
16.		Что такое LFSR?	ОПК-3 ОПК-7
17.		Как построить псевдослучайный генератор на основе регистра сдвига?	ОПК-3 ОПК-7
18.		На чем базируется стойкость генераторов псевдослучайных чисел, исследованных в лабораторной работе?	ОПК-3 ОПК-7
19.		Как реализовать возведение в степень чисел большой разрядности по большому модулю?	ОПК-3 ОПК-7
20.		Какая информация является конфиденциальной?	ОПК-3 ОПК-7
21.		Что относится к защищаемой информации?	ОПК-3 ОПК-7
22.		Что понимается под политикой безопасности?	ОПК-3 ОПК-7
23.		Что понимается под несанкционированным воздействием на защищаемую информацию?	ОПК-3 ОПК-7
24.		Дайте понятие конфиденциальности, целостности и доступности информации.	ОПК-3 ОПК-7
25.		Что такое симметричное шифрование?	ОПК-3 ОПК-7
26.		В чем особенность блочных шифров?	ОПК-3 ОПК-7
27.		В чем особенность асимметричных систем шифрования?	ОПК-3 ОПК-7
28.		На чем базируется криптостойкость RSA?	ОПК-3 ОПК-7
29.		Как увеличить производительность системы шифрования RSA?	ОПК-3 ОПК-7
30.		Составляющие функциональной безопасности	ОПК-3 ОПК-7
31.		Этапы построения систем безопасности	ОПК-3

			ОПК-7
32.		Назначение цифровой подписи.	ОПК-3 ОПК-7
33.		В чем отличие криптосхемы ЭльГамаля от RSA?	ОПК-3 ОПК-7
34.		Почему шифр RSA называется асимметричным?	ОПК-3 ОПК-7
35.		На чем основана стойкость шифра RSA?	ОПК-3 ОПК-7
36.		Что такое цифровой конверт?	ОПК-3 ОПК-7
37.		Опишите общую схему ЭЦП.	ОПК-3 ОПК-7
38.		Каково назначение хеш-функции?	ОПК-3 ОПК-7
39.		Какими свойствами противодействия должна обладать криптографическая хеш-функция?	ОПК-3
40.		Что такое MAC и как он формируется?	ОПК-7
41.		Какие тесты на случайность вам известны?	ОПК-3
42.		Сравните результаты тестов генераторов из первой лабораторной работы с тестами второй работы	ОПК-7
43.		Дайте определение информационной безопасности.	ОПК-3
44.		Какие цели и задачи включает в себя концепция национальной безопасности РФ?	ОПК-7
45.		Перечислите основные виды угроз информационной безопасности РФ.	ОПК-3

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 положениях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

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 студенту, если он:

Свободно и осознанно применяет базовые методы криптографической и антивирусной защиты информации при работе с корпоративными данными и документами в локальных и облачных хранилищах. Самостоятельно настраивает политики конфиденциальности и системы резервного копирования, обеспечивая надежную защиту в нестандартных ситуациях.

Безупречно оформляет отчеты о выполненной работе и списки литературы по действующему ГОСТу, используя офисное программное обеспечение. При публикации материалов в открытых источниках гарантированно обеспечивает защиту персональных данных, включая проверку и очистку метаданных файлов.

Проводит глубокий анализ требований к защите данных и всестороннее сравнение эффективности различных алгоритмов шифрования и хэширования. Выбор оптимального алгоритма и программно-аппаратных средств является полностью обоснованным с учетом заданных ограничений по производительности и криптостойкости для обеспечения конфиденциальности и целостности информации в разрабатываемой системе.

Оценка «хорошо» выставляется студенту, если он:

Уверенно применяет базовые методы и средства криптографической и антивирусной защиты при работе с корпоративными данными и документами в стандартных ситуациях. Понимает и соблюдает политики конфиденциальности, но при настройке защиты в нестандартных условиях может допускать незначительные технические ошибки, не влияющие на общий результат.

Правильно оформляет отчеты о выполненной работе и списки литературы по ГОСТу, используя офисное программное обеспечение. В основном соблюдает нормы информационной безопасности при подготовке презентаций и публикациях, однако возможны мелкие недочеты (например, в свойствах файла или оформлении второстепенных элементов).

Способен проанализировать требования к защите данных и провести сравнение основных характеристик популярных алгоритмов шифрования и хэширования. Обосновывает выбор адекватного алгоритма для обеспечения конфиденциальности и целостности информации, но сравнение может быть неполным или ограничиваться 2-3 очевидными параметрами.

Оценка «удовлетворительно» выставляется студенту, если он:

Имеет общее представление о базовых методах и средствах криптографической и антивирусной защиты информации. Способен применять их при работе с данными только по готовому шаблону или четкой инструкции (алгоритму), но затрудняется в самостоятельной настройке политик конфиденциальности и резервного копирования.

Демонстрирует умение оформлять отчеты и списки литературы, но с ошибками в оформлении по ГОСТу. Понимает необходимость защиты персональных данных, однако на практике при публикации материалов в открытых источниках может допускать их раскрытие из-за поверхностного контроля.

Знает названия и основные отличия (симметричные/асимметричные) некоторых криптографических алгоритмов, но не способен провести полноценный сравнительный анализ их эффективности. Затрудняется с обоснованным выбором оптимального алгоритма для решения конкретной задачи с учетом ограничений по производительности и криптостойкости.

Оценка «неудовлетворительно» выставляется студенту, если он:

Не знает базовых методов и средств криптографической и антивирусной защиты информации. Не умеет применять антивирусные средства, не понимает принципов резервного копирования и полностью игнорирует политики конфиденциальности при работе с корпоративными данными в локальных и облачных хранилищах.

Не владеет навыками оформления отчетов о выполненной работе и списков литературы в соответствии с требованиями ГОСТ. При подготовке презентаций или публикации материалов в открытых источниках полностью игнорирует нормы информационной безопасности, допуская раскрытие персональных данных.

Не ориентируется в видах криптографических алгоритмов и хэш-функций, не может привести их примеры и не понимает разницы между ними. Полностью отсутствует способность к анализу требований, сравнению и выбору средств защиты информации для реализации информационных систем.