

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Андреевна

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

Дата подписания: 17.06.2026 15:38:47

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619d42de79a7

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. Грובה
Ф.И.О.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Методы и средства криптографической защиты информации
название дисциплины (модуля)

Направление подготовки
Направленность (профиль)

10.03.01 «Информационная безопасность»
Организация и технологии защиты
информации (по отрасли или в сфере
профессиональной деятельности)

Год начала обучения

2026

Форма обучения

очная

Реализуется в семестре

5,6

Введение

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

2. ФОС является приложением к программе дисциплины (модуля) «Методы и средства криптографической защиты информации» в соответствии с образовательной программой высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

3. Разработчик: И.А. Калмыков, профессор кафедры информационной безопасности автоматизированных систем

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель Петренко В. И. - председатель УМК института цифрового развития.

Члены комиссии:

Плешенко В. С. – и.о. заведующего кафедрой информационной безопасности автоматизированных систем института цифрового развития;

Гиш Т. А. – доцент кафедры информационной безопасности автоматизированных систем института цифрового развития;

Представитель организации-работодателя _____
(Ф.И.О., должность)

Экспертное заключение: фонд оценочных средств соответствует образовательной программе по направлению подготовки, направленность (профиль) и рекомендуется для проведения текущего контроля успеваемости и промежуточной аттестации студентов

«____»_____

5. Срок действия ФОС определяется сроком реализации образовательной программы.

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

Уровни сформированности компетенци(ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
<i>Компетенция: ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;</i>				
Результаты обучения по дисциплине: <i>Индикатор: ИД-2_{ОПК-6}</i> <i>Эффективно применяет знания теории и методики курса при раскрытии компьютерных преступлений, при работе с конфиденциальной информацией и государственной тайной, при работе с организационно-правовым обеспечением, при работе с ЭП, при защите авторского и международного права, при проведении экспертизы преступлений в сфере компьютерной информации; применять нормативно-правовые акты</i>	Не знает основные принципы организации защиты информации ограниченного доступа при решении профессиональных задач в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Может раскрыть сущность только отдельных принципов организации защиты информации ограниченного доступа при решении профессиональных задач в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	Может пояснить практически всю методологию организации защиты информации ограниченного доступа при решении профессиональных задач в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	Применяет методологию организации защиты информации ограниченного доступа при решении профессиональных задач в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

при защите информации; оценивать состояние организационной защиты информации на объекте				
Компетенция: ОПК-9 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности				
Результаты обучения по дисциплине: <i>Индикатор: ИД-1_{ОПК-9}</i> Понимает базовые принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности.	Не знает основные принципы применения средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Может раскрыть сущность только отдельных основных этапов и принципов применения средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Может пояснить практически все основные этапы и принципы применения средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Выделяет все основные этапы и принципы применения средства криптографической и технической защиты информации для решения задач профессиональной деятельности
Результаты обучения по дисциплине: <i>Индикатор: ИД-2_{ОПК-9}</i> Использует средства криптографической и технической защиты информации для решения задач профессиональной деятельности.	Не знает основные средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Может раскрыть сущность только отдельных средств криптографической и технической защиты информации для решения задач профессиональной деятельности	Может пояснить практически все известные средства криптографической и технической защиты информации для решения задач профессиональной деятельности	применяет все известные средства криптографической и технической защиты информации для решения задач профессиональной деятельности
Результаты обучения по дисциплине: <i>Индикатор: ИД-3_{ОПК-9}</i> Выбирает оптимальный вариант использования навыков и методик применения	Не знает основные принципы и методологию применения средства криптографической и технической защиты информации для решения задач профессиональной	Может раскрыть сущность только отдельных принципов методологии применения средства криптографической и технической защиты информации для	Может пояснить практически всю методологию применения средства криптографической и технической защиты информации для решения задач	Использует методологию применения средства криптографической и технической защиты информации для

<i>средств криптографичес кой и технической защиты информации для решения задач профессиональн ой деятельности</i>	деятельности	решения задач профессионально й деятельности	профессиональн ой деятельности	решения задач профессиональн ой деятельности
--	--------------	--	-----------------------------------	--

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
		Основные понятия теории криптографической защиты информации	ОПК-9
		История криптографии	ОПК-9
		Классификация методов шифрования	ОПК-9
		Шифры подстановки. Криптоанализ шифров подстановки	ОПК-9
		Шифры перестановки. Криптоанализ шифров перестановки	ОПК-9
		Шифр Виженера.	ОПК-6
		Шифр Кардано.	ОПК-6
		Принципы построения блочных шифров	ОПК-6
		Петля Фейстеля	ОПК-6
		Американский стандарт шифрования DES. Основные показатели	ОПК-9
		Алгоритм шифрования DES	ОПК-9
		Ключевая система алгоритма DES	ОПК-6
		Практическое применение американского стандарта шифрования	ОПК-9

		DES. Двойной DES	ОПК-6
		Тройной DES	ОПК-9
		История конкурса на новый стандарт шифрования AES	ОПК-9
		Математические основы построения алгоритма AES	ОПК-9
		Основные элементы реализации шифра AES	ОПК-9
		Преобразования в алгоритме AES	ОПК-9
		Основные параметры отечественного стандарта шифрования Магма	ОПК-9
		Алгоритм шифрования Магма	ОПК-9
		Отечественный стандарт отечественного стандарта шифрования Кузнечик	ОПК-6
		Основные параметры алгоритма Кузнечик	ОПК-9
		Алгоритм шифрования Кузнечик	ОПК-6
		Принципы построения синхронных поточных систем шифрования	ОПК-6
		Схемные реализации синхронных поточных шифраторов. Генератор Фибоначчи.	ОПК-6
		Схемные реализации синхронных поточных шифраторов. Генератор на основе многотактовых кодовых фильтров	ОПК-9
		Принципы построения самосинхронизирующихся поточных систем	ОПК-9

		шифрования	
		Схемные реализации самосинхронизирующихся поточных шифраторов	ОПК-9
		Алгоритм поточного шифрования RC4	ОПК-9
		Режимы использования блочных шифров и их виды.	ОПК-9
		Режим электронной кодовой книги	ОПК-9
		Режим сцепления блоков шифрованного текста	ОПК-9
		Режим шифрования обратной связи (CFB)	ОПК-9
		Режим внешней обратной связи (OFB)	ОПК-9
		Режим счетчика	ОПК-9
		Надежность шифров	ОПК-9
		Энтропия и избыточность языка	ОПК-9
		Расстояние единственности	ОПК-9
		Теоретическая стойкость шифров	ОПК-9
		Практическая стойкость шифров	ОПК-9
		Основные принципы построения асимметричных систем шифрования	ОПК-9
		Алгоритм шифрования без передачи ключа	ОПК-9
		Алгоритм шифрования RSA	ОПК-9

		Алгоритм шифрования Эль-Гамала	ОПК-9
		Электронная цифровая подпись. Назначение. Функции ЭЦП.	ОПК-9
		Основные принципы построения электронной цифровой подписи	ОПК-9
		Цифровые подписи на основе шифрсистем с открытыми ключами	ОПК-9
		Электронная цифровая подпись на основе RSA	ОПК-9
		Электронная цифровая подпись на основе алгоритма Эль-Гамала	ОПК-9
		Управление ключами. Двухсторонние протоколы	ОПК-9
		Управление ключами. Трехсторонние протоколы	ОПК-9
		Метод экспоненциального ключевого обмена на основе алгоритма	ОПК-9
		Диффи-Хеллмана.	ОПК-9
		Алгоритм односторонней генерации ключа Диффи-Хеллмана	ОПК-9
		Модификация алгоритма Диффи-Хеллмана	ОПК-9
		Криптографические схемы разделения секрета. Виды схем разделения секрета.	ОПК-9
		Основные принципы построения схем разделения секрета	ОПК-9
		Схема разделения секрета Шамира	ОПК-9
		Протоколы аутентификации. Назначение. Классификация протоколов аутентификации	ОПК-9

		Парольная аутентификация	ОПК-9
		Аутентификация методом "запрос-ответ"	ОПК-9
		Протоколы аутентификация, основанные на доказательствах с нулевым разглашением	ОПК-9
		Скрытый канал. Назначение. Решаемые задачи.	ОПК-9
		Построение скрытого канала на основе схемы Онга-Шнорра-Шамирах	ОПК-9
		Построение скрытого канала на основе схемы Эль-Гамала	ОПК-9
		Криптографические хеш-функции. Назначение хеш-функции. Свойства хеш-функции	ОПК-9
		Функции хеширования и целостность данных	ОПК-9
		Бесключевые функции хеширования	ОПК-9
	a,d	Какой из указанных адресов может быть использован в качестве шлюза по умолчанию для сети 172.19.255.0/25? +: 172.19.255.126 -:172.19.255.128 -:172.19.255.129 +: 172.19.255.16 -: 172.19.255.130	ОПК-9
	a,b,c	Какой из указанных адресов может быть использован в качестве	ОПК-9

		шлюза по умолчанию для сети 172.16.8.0/22? +: 172.16.8.2 +: 172.16.11.1 +: 172.16.10.255 -. 172.16.12.1 -. 172.16.12.255	
	a	Какой префикс маски подсети необходимо использовать для выделения единого с точки зрения маршрутизации адресного пространства 1039 рабочим станциям? +: /21 -. /22 -. /30 -. /24	ОПК-9
	c	Какой префикс маски подсети необходимо использовать для выделения единого с точки зрения маршрутизации адресного пространства 511 рабочим станциям? -. /24 -. /26 +: /22 -. /23	ОПК-9
	b,d	Какой префикс маски подсети необходимо использовать для	ОПК-9

		выделения единого с точки зрения маршрутизации адресного пространства не менее чем 127 рабочим станциям? -: /26 +: /24 -: /25 +: /22	
	a,b,e	Выберите функции, которые выполняет коммутатор L2 в локальной сети +: принимает, обрабатывает и пересылает Ethernet-кадры +: обеспечивает тиражирование и рассылку широковещательных кадров -: обрабатывает заголовки сетевого и транспортного уровней -: выполняет конфигурирование сетевых устройств для сегментации топологии физического уровня на выделенные (изолированные) сегменты +: обеспечивает функционирование протоколов и технологий для реализации отказоустойчивой топологии сети	ОПК-9
	c,d	Выберите функции, которые выполняет концентратор в локальной сети -: разделяет сеть на изолированные сегменты -: обеспечивает возможность функционирования физических	ОПК-9

		подключений в режиме Full-Duplex +: обеспечивает возможность функционирования физических подключений в режиме Half-Duplex +: выполняет ретрансляцию электрических сигналов между интерфейсами -: выполняет анализ заголовков канального уровня	
	a,c,d	Выберите из приведенного списка недостатки использования в сети концентраторов +: не разделяет сеть на домены коллизий -: отсутствие блокировки распространения broadcast трафика +: отсутствие блокировки неконтролируемого распространения unicast трафика +: отсутствует возможность анализа заголовков протоколов канального уровня -: отсутствует возможность анализа заголовков протоколов прикладного уровня	ОПК-9
	abf	Выберите функции, которые выполняет маршрутизатор L3 в локальной сети +: выполняет анализ заголовков протоколов канального уровня +: выполняет анализ заголовков протоколов сетевого уровня -: выполняет анализ заголовков протоколов прикладного уровня	ОПК-9

		-: выполняет блокировку пересылки IP пакетов между подсетями в локальной сети -: выполняет блокировку пересылки IP пакетов между локальной сетью и публично доступными сетями +: формирует таблицу маршрутизации на основе конфигурационных параметров и информации от протоколов динамической маршрутизации	
	b	Какой адрес сети из приведенных ниже содержит в себе адреса сетей 10.8.0.0/25, 10.8.0.128/26, 10.8.1.0/24, 10.8.2.128/25? -: 10.8.0.0/24 +: 10.8.0.0/22 -: 10.8.0.0/23 -: 10.8.1.0/24	ОПК-9
	a	Какой адрес сети из приведенных ниже содержит в себе адреса сетей 10.100.1.0/26, 10.100.0.128/25, 10.100.3.0/24, 10.100.2.192/27? +: 10.100.0.0/22 -: 10.100.0.0/24 -: 10.100.0.0/23 -: 10.100.2.0/23	ОПК-9
	ad	Какие адреса сетей из приведенных ниже содержат в себе все адреса	ОПК-9

		сетей 45.128.4.0/22, 45.128.16.0/21, 45.128.1.0/24, 45.128.3.128/30? +: 45.128.0.0/19 -: 45.128.0.0/22 -:45.128.0.0/21 +:45.128.0.0/16	
	с	Какое максимальное количество уникальных сетей с префиксом маски /25 можно получить, разделяя сеть 10.0.0.0/8? -: 256 -:65536 +: 131072 -: 16777216	ОПК-9
	а	Какое максимальное количество уникальных сетей с префиксом маски /26 можно получить, разделяя сеть 172.16.0.0/22? +: 16 -: 256 -: 1024 -: 4	ОПК-9
	б	Какое максимальное количество уникальных сетей с префиксом маски /22 можно получить, разделяя сеть 62.16.128.0/17?	ОПК-9

		-: 256 +: 32 -: 64 -: 16	
	a	Какое максимальное количество уникальных сетей с префиксом маски /30 можно получить, разделяя сеть 10.255.255.0/24? +: 64 -: 32 -: 256 -: 8	ОПК-9
	b	Какое максимальное количество уникальных сетей с префиксом маски /29 можно получить, разделяя сеть 10.90.0.0/19? -: 512 +: 1024 -: 65536 -: 4096	ОПК-9
	a	Можно ли разделить сеть 192.168.32.0/21 таким образом, чтобы получились три уникальных сети с префиксом маски /24, пять сетей с префиксом /26 и семь сетей с префиксом /29?	ОПК-9

		+: да, можно -: нет, невозможно	
	b	Можно ли разделить сеть 192.168.32.0/22 таким образом, чтобы получились три уникальных сети с префиксом маски /24, пять сетей с префиксом /26 и семь сетей с префиксом /29? -: да, можно +: нет, невозможно	ОПК-9
	b	Можно ли разделить сеть 192.168.64.0/23 таким образом, чтобы получились две уникальные сети с префиксом маски /24, три сети с префиксом /26 и семь сетей с префиксом /29? -: да, можно +: нет, невозможно	ОПК-9
	a	Можно ли разделить сеть 192.168.0.0/24 таким образом, чтобы получились три уникальных сети с префиксом маски /27, пять сетей с префиксом /29 и шесть сетей с префиксом /30? +: да, можно -: нет, невозможно	ОПК-9
	a	Можно ли разделить сеть 192.168.64.0/21 таким образом, чтобы получились пять уникальных сети с префиксом маски /24, восемь сетей с префиксом /26 и восемь сетей с префиксом /29? +: да, можно	ОПК-9

		-: нет, невозможно	
	b	Является ли передача данных между двумя узлами сети по протоколу IP взаимодействием с установлением соединения? -: да +: нет	ОПК-9
	c	Что содержит поле «Protocol» в заголовке IP пакета? -: Код протокола, который передает маршрутную информацию -: Код протокола, который необходимо использовать для передачи данных в данном пакете +: Код протокола, который инкапсулируется в IP пакет -: Версию протокола транспортного уровня	ОПК-9
	b	Проверку на целостность какой части IP пакета включает в себя расчет контрольной суммы? -: только данных +: только заголовка -: заголовка и данных -: заголовка верхнего уровня	ОПК-9
	abc	Каким образом формируется информация об IP адресе назначения? +: пользователь или программное обеспечение используют IP адрес в	ОПК-9

		качестве исходных данных, т.е. знают его заранее +: IP адрес назначения может содержаться в ответе DNS сервера +: IP адрес назначения может содержаться в ответе на RARP запрос -: IP адрес назначения может содержаться в ответе на ARP запрос	
	а	Для каких целей используется флаг «SYN»? +: для установления TCP соединения -: для указания на срочность доставки информации, содержащейся в TCP сегменте -: для информирования приемной стороны об атаке -: для восстановления неожиданно разорванного соединения	ОПК-9
	с	Для каких целей используется флаг «FIN»? -: для восстановления неожиданно разорванного соединения -: для указания на повторно передаваемые данные +: для информирования удаленной стороны о завершении соединения -: о переключении на финский язык	ОПК-9
	а	Для каких целей используется флаг «RST»? +: для аварийного разрыва соединения	ОПК-9

		-: для информирования приемной стороны об атаке -: для восстановления неожиданно разорванного соединения -: для указания на повторно передаваемые данные	
	b	Если принятый TCP сегмент содержит значения полей заголовка Sequence Number (SN) – 544, Acknowledgment Number (ACK NUM) – 298 и 152 байт данных. Что принимающая станция укажет в ответном TCP сегменте в поле ACK NUM? -: 451 +: 697 -: 450 -: 696 -: нет правильного ответа	ОПК-9

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 (в соответствии с результатами освоения дисциплины)

Оценка «отлично» выставляется студенту, если студент дал полный, развернутый ответ на поставленные вопросы, при этом показана совокупность осознанных знаний по теме дисциплины, доказательно раскрыты основные положения вопроса; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий. Ответ изложен литературным языком с использованием технической терминологии. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа. Ситуационная задача по теме решена правильно. *Оценка «отлично» выставляется студенту*, если он обладает прочным и аргументированным всесторонним пониманием основных принципов работы средств криптографической защиты информации, способен обоснованно выбрать и применить их при решении задач профессиональной деятельности. Компетенция ОПК-10 освоена на высоком уровне.

Оценка «хорошо» выставляется студенту, если студент дал полный, развернутый ответ на поставленные вопросы, при этом показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком с использованием технической терминологии. Могут быть допущены 2-3 неточности или незначительные ошибки, исправленные студентом с помощью преподавателя. Ситуационная задача по теме решена правильно, но при ее решении допущено не более одной ошибки. *Оценка «хорошо» выставляется студенту*, если он, может пояснить практически все базовые понятия, которые положены в основу принципов построения средств криптографической и технической защиты информации, и обосновать целесообразность их применения для решения задач профессиональной деятельности. Компетенция ОПК-10 освоена на среднем уровне

Оценка «удовлетворительно» выставляется студенту, если студент дал недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано. Речевое оформление требует поправок, коррекции. Ситуационная задача по теме решена правильно, но при ее решении допущено не более двух ошибок. *Оценка «удовлетворительно» выставляется студенту*, если он может раскрыть сущность только отдельных принципов построения средств криптографической и технической защиты информации и обосновать эффективность их применения для решения задач профессиональной деятельности. Компетенция ОПК-10 освоена на минимальном уровне

Оценка «неудовлетворительно» выставляется студенту, если ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь обсуждаемого вопроса с другими вопросами темы. Отсутствуют выводы, конкретизация и

доказательность изложения. Речь неграмотная, терминология не используется. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента, или ответ на вопрос полностью отсутствует или студент отказался от ответа. Ситуационная задача по теме решена неправильно. *Оценка «неудовлетворительно»* выставляется студенту, если он не понимает основные принципы построения средств криптографической и технической защиты информации, не может пояснить их сущность и обосновать их применение для решения задач профессиональной деятельности. Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, компетенция ОПК-10 не сформирована.