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
Криптографические протоколы

Специальность	10.05.01 Компьютерная безопасность
Специализация	Информационно-аналитическая и техническая экспертиза компьютерных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	7

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Криптографические протоколы». 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 (модуля) «Криптографические протоколы»

3. Разработчик: Свистунов Николай Юрьевич, ассистент кафедры вычислительной математики и кибернетики

4. Проведена экспертиза ФОС.
Члены экспертной группы:

Председатель Бабенко М.Г., заведующий кафедрой вычислительной математики и кибернетики

Члены комиссии: Тебуева Ф.Б., профессор кафедры вычислительной математики и кибернетики
Гусева Л.Л., доцент кафедры вычислительной математики и кибернетики
Представитель организации-работодателя: Березницкий А.С., главный аналитик федерального государственного бюджетного учреждения «Кабардино-Балкарская лаборатория судебной экспертизы Министерства юстиции Российской Федерации».

Экспертное заключение: Представленный ФОС по дисциплине «Криптографические протоколы» соответствует требованиям ФГОС ВО. Предлагаемые преподавателем формы и средства текущего контроля адекватны целям и задачам реализации образовательной программы высшего образования по специальности 10.05.01 Компьютерная безопасность, а также целям и задачам рабочей программы реализуемой учебной дисциплины. Оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации представлены в полном объеме.

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 компетенции(ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (неудовлетвори-тельно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ОПК-10				
Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-2$_{ОПК-10}$ конфигурирует средства криптографической защиты информации	Не способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	Способен на базовом уровне анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	Способен на хорошем уровне анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности. Обладает расширенными знаниями о криптографических протоколах и порядке их применения

Оценочные средства для проверки уровня сформированности компетенций
7 семестр

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1	участников агентов сторон	Отличие криптографического протокола от криптографического алгоритма состоит в наличии нескольких взаимодействующих ___	ОПК-10
2	симметричных	В ___ системах шифрования каждый ключ шифрования совпадает с соответствующим ему ключом дешифрования	ОПК-10
3	асимметричных	В ___ системах шифрования ключ шифрования и соответствующий ему ключ дешифрования, как правило, различны	ОПК-10
4	б) электронной подписи	Закрытый ключ используется для зашифрования данных, а открытый ключ – для их расшифровывания в алгоритмах: а) генерации общего сеансового ключа б) электронной подписи в) выработки имитовставки г) доказательства с нулевым разглашением	ОПК-10
5	Односторонняя	___ функция – это функция, для которой не существует быстрого алгоритма нахождения аргумента по известному выходному значению	ОПК-10

6	сообщение	В терминологии криптографических протоколов ___ – это любой объект, который один из участников передаёт другому в процессе функционирования протокола	ОПК-10
7	нонс nonce	Псевдослучайное число, генерируемое участником криптографического протокола, называется ___	ОПК-10
8	доказательства с нулевым разглашением идентификации с нулевым разглашением	Протоколы, позволяющие подтвердить знание агентом некоторого секрета таким образом, чтобы никакая информация о секрете не была разглашена проверяющей стороне, называются протоколами _	ОПК-10
9	Криптографические примитивы	___ – это математические конструкции и алгоритмы, которые используются в качестве элементарных компонентов при построении криптографических протоколов	ОПК-10
10	Слепая	___ электронная подпись – это электронная подпись, выполненная таким образом, что подписывающий агент не получает никакой информации о подписываемом сообщении	ОПК-10
11	г) совместной генерации секретного ключа	Протокол Диффи-Хеллмана предназначен для: а) подписывания сообщений б) аутентификации агентов в) доказательства знания секрета без его разглашения г) совместной генерации секретного ключа	ОПК-10
12	б) протокол Эль-Гамаля	К протоколам аутентификации НЕ относится: а) протокол Фейге-Фиата-Шамира б) протокол Эль-Гамаля в) протокол Нидхема-Шрёдера г) протокол Шаума	ОПК-10
13	20	Какое количество целей, характеризующих безопасность криптографических протоколов, выделяет Инженерный совет Интернета (IETF)?	ОПК-10
14	человек посередине	Вид атаки, при которой злоумышленник встраивается в канал информационного обмена и способен вносить изменения в сообщения и перенаправлять их, называется ___	ОПК-10
15	интерактивным	Криптографический протокол называется ___, если участники осуществляют взаимный обмен сообщениями, а не только однократную передачу	ОПК-10

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».

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 на высоком уровне способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности. Обладает расширенными знаниями о криптографических протоколах и порядке их применения.

Оценка «хорошо» выставляется студенту, если он на среднем уровне способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

Оценка «удовлетворительно» выставляется студенту, если он на минимальном уровне способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

Оценка «неудовлетворительно» выставляется студенту, если он в недостаточной степени способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.