МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ
Зам. директора по учебной работе
Пятигорского института (филиал)
СКФУ
_____ М.В. Мартыненко
«28» марта 2022 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине **«Методы и средства криптографической защиты информации»**

Направление подготовки **10.03.01 Информационная безопасность**
Направленность (профиль) **Безопасность компьютерных систем**
Форма обучения очная
Год начала обучения 2022
Реализуется в 5, 6 семестрах

Предисловие

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Методы и средства криптографической защиты информации». Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информацию 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 «Методы и средства криптографической защиты информации» в соответствии с образовательной программой высшего образования по направлению подготовки 10.03.01 Информационная безопасность

3. Разработчик: Битюцкая Наталья Ивановна, доцент кафедры систем управления и информационных технологий, кандидат физ.-мат. наук, доцент

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:
Цаплева В.В.– и.о. зав. кафедрой систем управления и информационных технологий

Члены комиссии:
Флоринский О.С. – доцент кафедры систем управления и информационных технологий
Мишин В.В.– доцент кафедры систем управления и информационных технологий

Представитель организации-работодателя:
Афанасов Владимир Христофорович - директор ООО «Сателлит»

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.03.01 Информационная безопасность и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Методы и средства криптографической защиты информации».
28 марта 2022 г.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код оцениваемой компетенции, индикатора (ов)	Этап формирования компетенции (№ темы) *(в соответствии с рабочей программой дисциплины)*	Средства и технологии оценки	Вид контроля, аттестация *(текущий /промежуточный)*	Тип контроля *(устный, письменный или с использованием технических средств)*	Наименование оценочного средства
5 семестр					
ОПК-3	1 - 10	собеседование	текущий	устный	Вопросы для собеседования
ОПК-7 ОПК-9	11 - 31	собеседование	текущий	устный	Вопросы для собеседования
ПК-4	32 - 34	собеседование	текущий	устный	Вопросы для собеседования
6 семестр					
ОПК-7 ОПК-9	11 - 31	собеседование	текущий	устный	Вопросы для собеседования
ПК-4	32 - 34	собеседование	текущий	устный	Вопросы для собеседования
ОПК-3 ОПК-7 ОПК-9 ПК-4	1 - 34	экзамен	промежуточный	устный	Вопросы к экзамену

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

Уровни сформированности компетенций (индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (Неудовлетворительно)	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов

	2 балла			
Компетенция:ОПК-3				
Результаты обучения по дисциплине (модулю): *Индикатор:* **ИД-1**$_{\text{опк-3}}$ Знает необходимые математические методы для решения задач обеспечения защиты информации. **ИД-2**$_{\text{опк-3}}$ Умеет применять совокупность необходимых математических методов для решения задач обеспечения защиты информации. **ИД-3**$_{\text{опк-3}}$ Имеет навыки применения необходимых математических методов для решения задач обеспечения защиты информации.	Не знает необходимые математически е методы для решения задач обеспечения защиты информации Не умеет применять совокупность необходимых математически х методов для решения задач обеспечения защиты информации. Не имеет навыков применения необходимых математически х методов для решения задач обеспечения защиты информации.	Недостаточно хорошо знает необходимые математическ ие методы для решения задач обеспе-чения защиты информации Плохо умеет применять совокупность необходимых математическ их методов для решения задач обеспечения защиты информации. Не в полной мере владеет навыками применения необходимых математическ их методов для решения задач обеспечения защиты информации.	Хорошо знает необходимые математически е методы для решения задач обеспечения защиты информации. Умеет применять совокупность необходимых математически х методов для решения задач обеспечения защиты информации. В основном владеет навыками применения необходимых математически х методов для решения задач обеспечения защиты информации.	Отлично знает необходимые математические методы для решения задач обеспечения защиты информации. Отлично умеет применять совокупность необходимых математических методов для решения задач обеспечения защиты информации. В совершенстве владеет навыками применения необходимых математических методов для решения задач обеспечения защиты информации.
Компетенция: ОПК-7				
Результаты обучения по дисциплине (модулю): *Индикатор:* **ИД-1**$_{\text{опк-7}}$ Знает языки	Не знает языки программирова	Слабо знает языки программиро вания и системы отки ммных	Хорошо знает языки программиров ания и системы разработки программных	Отлично знает языки программирова ния и системы разработки программных

средств для решения профессиональных задач. **ИД-2**$_{\text{опк-7}}$ Способен выбирать необходимые языки програм-мирования и системы разработки программных средств для решения профессиональных задач. **ИД-3**$_{\text{опк-7}}$ Имеет навыки применения языков программировани я и систем разработки программных средств для решения профессиональны х задач.	решения профессиональ ных задач. Не способен выбирать необходимые языки програм-мирования и системы разработки программных средств для решения профессиональ ных задач. Не применяет языки программирова ния и системы разработки программных средств для решения профессиональ ных задач.	средств для решения профессионал ьных задач. Недостаточно хорошо умеет выбирать необходимые языки програм-мирования и системы разработки программных средств для решения профессионал ьных задач. Имеет небольшие навыки применения языков программиро вания и систем разработки программных средств для решения профессионал ьных задач.	средств для решения профессиональ ных задач. Способен выбирать необходимые языки програм-мирования и системы разработки программных средств для решения профессиональ ных задач. Имеет навыки применения языков программиров ания и систем разработки программных средств для решения профессиональ ных задач.	средств для решения профессиональн ых задач. Отлично умеет выбирать необходимые языки програм-мирования и системы разработки программных средств для решения профессиональн ых задач. Имеет отличные навыки применения языков программирова ния и систем разработки программных средств для решения профессиональн ых задач.
Компетенция: ОПК-9				
Результаты обучения по дисциплине (модулю): *Индикатор:* **ИД-1**$_{\text{опк-9}}$ Знает криптографически е алгоритмы в современных программных комплексах. **ИД-2**$_{\text{опк-9}}$ Умеет устанавливать причины, цели и условия изменения	Не знает криптографиче ские алгоритмы в современных программных комплексах. Не умеет устанавливать причины, цели и условия	Слабо знает криптографи ческие алгоритмы в современных программных комплексах. Недостаточно хорошо умеет устанавливат ь причины,	Хорошо знает криптографиче ские алгоритмы в современных программных комплексах. Хорошо умеет устанавливать причины, цели и условия	В совершенстве знает криптогра-фические алгоритмы в современных программных комплексах. Отлично умеет устанавливать причины, цели

свойств алгоритмов и протоколов применительно к конкретным условиям. **ИД-3$_{ОПК-9}$** Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	изменения свойств алгоритмов и протоколов применительно к конкретным условиям. Не владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. Слабо владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	изменения свойств алгоритмов и протоколов применительно к конкретным условиям. Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. В совершенстве владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.
Компетенция: ПК-4				
Результаты обучения по дисциплине (модулю): *Индикатор:* **ИД-1$_{ПК-4}$** Знает методы комплексного подхода в организации политики информационной безопасности. **ИД-2$_{ПК-4}$** Умеет формулировать, настраивать политики безопасности. **ИД-3$_{ПК-4}$** Владеет навыками формулирования и контролирования соблюдения требований политики безопасности	Не знает методы комплексного подхода в организации политики информационной безопасности. е умеет формулировать, настраивать политики безопасности. Не владеет навыками	Слабо знает методы комплексного подхода в организации политики информационной безопасности. Недостаточно хорошо умеет формулировать, настраивать политики безопасности. Слабо владеет навыками лирова	Хорошо знает методы комплексного подхода в организации политики информационной безопасности. Хорошо умеет формулировать, настраивать политики безопасности. Владеет навыками формулирования и контролирования соблюдения требований политики	В совершенстве знает методы комплексного подхода в организации политики информационной безопасности. Отлично умеет формулировать, настраивать политики безопасности. В совершенстве владеет навыками формулирования и контролирования соблюдения требований

	требований политики безопасности.	соблюдения требований политики безопасности.	безопасности.	политики безопасности.

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

Рейтинговая оценка знаний студента (в случаях, предусмотренных нормативными актами СКФУ).

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
1.	Собеседование по темам 1-4. Защита лабораторных работ	8 неделя	25
2.	Собеседование по теме 5-8, 13. Защита лабораторных работ	16 неделя	30
	Итого за 5семестр		**55**
3.	Собеседование по темам 19, 21, 24. Защита лабораторных работ	7 неделя	25
4.	Собеседование по темам 25, 29-33. Защита лабораторных работ	14 неделя	30
	Итого за 6 семестр		**55**
	Итого		**110**

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	***Рейтинговый балл (в % от максимального балла за контрольное задание)***
Отличный	***100***
Хороший	***80***
Удовлетворительный	***60***
Неудовлетворительный	***0***

Промежуточная аттестация

Промежуточная аттестация в 5 семестре проводится в форме **зачета с оценкой**.

Процедура зачета как отдельное контрольное мероприятие не проводится, оценивание знаний обучающегося происходит по результатам текущего контроля.

Зачет выставляется по результатам работы в семестре, при сдаче всех контрольных точек, предусмотренных текущим контролем успеваемости. Если по итогам семестра обучающийся набрал менее 60 баллов, ему ставится отметка «зачтено». Обучающемуся, набравшему менее 33 баллов, ставится отметка «не зачтено».

Количество баллов за зачет ($S_{зач}$) при различных рейтинговых баллах

по дисциплине по результатам работы в семестре

Рейтинговый балл по дисциплине по результатам работы в семестре ($R_{сем}$)	**Количество баллов за зачет ($S_{зач}$)**
$50 \leq R_{сем} \leq 60$	**40**
$39 \leq R_{сем} < 50$	**35**
$33 \leq R_{сем} < 39$	**27**
$R_{сем} < 33$	**0**

Промежуточная аттестация в 6 семестре проводится в форме **экзамена,** предусматривает проведение обязательной экзаменационной процедуры и оценивается 40 баллами из 100. Минимальное количество баллов, необходимое для допуска к экзамену, составляет 33 балла. Положительный ответ студента на экзамене оценивается рейтинговыми баллами в диапазоне от **20** до **40** (**$20 \leq S_{экз} \leq 40$**), оценка **меньше 20** баллов считается неудовлетворительной.

Шкала соответствия рейтингового балла экзамена 5-балльной системе

Рейтинговый балл по дисциплине	**Оценка по 5-балльной системе**
35 – 40	Отлично
28 – 34	Хорошо
20 – 27	Удовлетворительно

Итоговая оценка по дисциплине, изучаемой в одном семестре, определяется по сумме баллов, набранных за работу в течение семестра, и баллов, полученных при сдаче экзамена:

Шкала пересчета рейтингового балла по дисциплине
в оценку по 5-балльной системе

Рейтинговый балл по дисциплине	**Оценка по 5-балльной системе**
88 – 100	Отлично
72 – 87	Хорошо
53 – 71	Удовлетворительно
< 53	Неудовлетворительно

3. Типовые контрольные задания и иные материалы, характеризующие этапы формирования компетенций

Вопросы к экзамену
по дисциплине МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

6 семестр

Базовый уровень

Вопросы (задача, задание) для проверки уровня обученности.

Знать

1. Основные понятия в области криптографии.
2. Классификация классических шифров: шифры замены и перестановки, моноалфавитные и многоалфавитные шифры.
3. Классические шифры с симметричным ключом. Шифры замены: аддитивные, мультипликативные, аффинные, автоключевой, Виженера,

Плейфера, Хилла, роторный, одноразового блокнота.

4. Классические шифры перестановки: бесключевой шифр, ключевые шифры и шифры с двойной перестановкой.

5. Современные блочные шифры с симметричным ключом. Основные компоненты современного блочного шифра. Шифры Фейстеля и не-Фейстеля.

6. Современные поточные шифры с симметричным ключом. Синхронные и несинхронные шифры потока. Преимущества и проблемы современных шифров потока.

7. Современный стандарт шифрования (DES). Структура шифра DES. Раунды шифрования. Функция DES. Генерация ключей раундов.

8. Усовершенствованный стандарт шифрования (AES). Алгоритм расширения ключей. Анализ расширения ключа. Алгоритмы шифрования и дешифрования в AES.

9. Российский стандарт ГОСТ 2847-89, особенности, принципы построения, методы шифрования.

10. Алгоритмы шифрования с открытыми ключами. Концепция криптографии с открытым ключом. Криптосистема RSA. Стойкость RSA.

11. Алгоритмы генерации простых чисел. Проверка чисел на простоту. Способы проверки на простое число. Решето Эратосфена. Phi-функция Эйлера. Простые числа Мерсенны. Простые числа Ферма. Детерминированные и вероятностные алгоритмы проверки чисел на простоту.

12. Сложность криптографических алгоритмов. Понятие сложности алгоритма. Линейная, полиномиальная и неполиномиальная сложность. Класс NP – полных задач.

13. Криптосистемы с открытым ключом. Криптосистема Рабина. Криптосистема Эль-Гамаля. Алгоритмы шифрования, дешифрования и генерации ключей в криптосистемах Рабина и Эль-Гамаля. Безопасность данных криптосистем.

14. Аутентификация данных. Электронная цифровая подпись. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.

15. Алгоритмы ЭЦП: RSA, Эль-Гамаля, ФиатаШамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ванАнтверпена.

16. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.9.

17. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля. Алгоритм формирования схемы Эль-Гамаля. Алгоритм формирования цифровой подписи. Проверка подписи.

18. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Парольные схемы и протоколы "рукопожатия".

19. Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации.

Уметь

1. Шифровать тексты с помощью классических шифров.
2. Шифровать двоичные последовательности с помощью современных шифров.
3. Проверять требования к криптосистемам.
4. Использовать перестановки, подстановки и их комбинации.
5. Реализовывать криптографические методы.

Владеть

1. Методами управления ключами.
2. Методами генерации, накопления и распределения ключей.
3. Основами знаний по порядку разработки схемы ЭЦП Рабина.
4. Основами знаний по порядку разработки схемы ЭЦП Диффи - Хэллмана.
5. Основами знаний по порядку разработки схемы ЭЦП Эль-Гамаля.

Повышенный уровень

Вопросы (задача, задание) для проверки уровня обученности.

Знать
1. Виды атак криптоанализа. Способы противодействия им.
2. Криптоанализ шифров замены.
3. Криптоанализ шифров перестановки.
4. Атаки на современные блочные шифры.
5. Криптоанализ современных шифров потока.
6. Двукратный и трехкратный DES. Криптоанализ шифра DES.
7. Анализ AES.
8. Виды атак на RSA.
9. Способы определения сложности алгоритмов.
10. Сложность известных алгоритмов, используемых в криптографии и криптоанализе.
11. Криптосистемы на основе метода эллиптических кривых.
12. Безопасность криптосистемы с эллиптической кривой.
13. Атаки на криптографические протоколы. Виды атак, способ подмены пользователя сети, способ замены долговременного ключа.
14. Способы отражения атак на криптографические протоколы.

Уметь
1. Отражать атаки на криптографические протоколы.
2. Выбирать правильно параметры для шифрования наиболее известными шифрами.
3. Оценивать криптостойкость алгоритма шифрования.

Владеть
1. Способами построения криптографических протоколов.
2. Способами отражения атак на криптографические протоколы.

1. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если теоретическое содержание курса освоено полностью, без пробелов; исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует в ответе дополнительный материал, все предусмотренные программой задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному; анализирует полученные результаты; проявляет самостоятельность при выполнении заданий.

Оценка «хорошо» выставляется студенту, если теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

Оценка «удовлетворительно» выставляется студенту, если теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки, при ответе на поставленный вопрос студент допускает неточности, недостаточно

правильные формулировки, наблюдаются нарушения логической последовательности в изложении программного материала.

Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, необходимые практические компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному.

2. Описание шкалы оценивания

Промежуточная аттестация в форме **экзамена** предусматривает проведение обязательной экзаменационной процедуры и оценивается 45 баллами из 100. Минимальное количество баллов, необходимое для допуска к экзамену, составляет 33 балла. Положительный ответ студента на экзамене оценивается рейтинговыми баллами в диапазоне от **20** до **45** (**$20 \leq S_{экз} \leq 45$**), оценка **меньше 20** баллов считается неудовлетворительной.

Шкала соответствия рейтингового балла экзамена 5-балльной системе

Рейтинговый балл по дисциплине	**Оценка по 5-балльной системе**
37 – 45	Отлично
28 – 36	Хорошо
20 – 27	Удовлетворительно

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения **экзамена** осуществляется в соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования в СКФУ.

В экзаменационный билет включаются два теоретических вопроса базового и один повышенного уровня.

Для подготовки по билету отводится от 40 до 60 минут.

При подготовке к ответу студенту предоставляется право пользования собственными лекциями, а также любой справочной литературой в течение 3-5 минут.

Составитель _____ Н.И. Битюцкая

«____»_____20 г.

Вопросы для собеседования
по дисциплине МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

5 семестр
Базовый уровень

1. Основные понятия криптографии.
2. Наиболее известные классические шифры замены.
3. Наиболее известные классические шифры перестановки.
4. Принципы построения современных блочных шифров с симметричным ключом.
5. Основные компоненты современного блочного шифра.
6. Шифры Фейстеля и не-Фейстеля.
7. Принципы построения современных поточных шифров с симметричным ключом. Синхронные и несинхронные шифры потока.
8. Преимущества и проблемы современных шифров потока.
9. Современный стандарт шифрования (DES). Структура шифра DES. Раунды шифрования. Функция DES. Генерация ключей раундов.
10. Алгоритм расширения ключей. Анализ расширения ключа. Алгоритмы шифрования и дешифрования в AES.
11. Алгоритмы шифрования и дешифрования в российском стандарте ГОСТ 28147-89.
12. Концепция криптографии с открытым ключом.
13. Криптосистема RSA.

Повышенный уровень

1. Виды атак криптоанализа. Способы противодействия им.
2. Криптоанализ шифров замены.
3. Криптоанализ шифров перестановки.
4. Атаки на блочные шифры.
5. Криптоанализ шифров потока.
6. Двукратный и трехкратный DES.
7. Криптоанализ шифра DES.
8. Анализ AES.
9. Стойкость RSA. Виды атак на RSA.

6 семестр
Базовый уровень

1. Алгоритмы генерации простых чисел.
2. Способы проверки на простое число. Решето Эратосфена.
3. Phi-функция Эйлера. Простые числа Мерсенны. Простые числа Ферма.
4. Детерминированные и вероятностные алгоритмы проверки чисел на простоту.
5. Понятие и оценка сложности криптографических алгоритмов.
6. Криптосистема Рабина.
7. Криптографическая система Эль-Гамаля.
8. Алгоритмы шифрования, дешифрования и генерации ключей в криптосистемах Рабина и Эль-Гамаля.
9. Понятие электронной цифровой подписи и требования к ней.
10. Алгоритмы ЭЦП: RSA, Эль-Гамаля.
11. Алгоритмы ЭЦП: ФиатаШамира, Онга-Шнорра-Шамира.
12. Неотрицаемая подпись Шаума-ванАнтверпена.
13. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля.
14. Понятие криптографического протокола. Основные примеры.
15. Связь стойкости протокола со стойкостью базовой криптографической системы.
16. Классификация криптографических протоколов.
17. Парольные схемы и протоколы "рукопожатия".

18. Взаимосвязь между протоколами аутентификации и цифровой подписи.
19. Протоколы сертификации ключей.
20. Протоколы предварительного распределения ключей.
21. Протоколы выработки сеансовых ключей.
22. Открытое распределение ключей Диффи-Хеллмана и его модификации.

Повышенный уровень

1. Способы определения сложности алгоритмов.
2. Сложность известных алгоритмов, используемых в криптографии и криптоанализе.
3. Криптосистемы на основе метода эллиптических кривых.
4. Атаки и угрозы схемам ЭЦП.
5. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.
6. Атаки на криптографические протоколы. Виды атак, способ подмены пользователя сети, способ замены долговременного ключа.
7. Способы отражения атак на криптографические протоколы.

1. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если он в ходе собеседования правильно ответил на вопрос по теме собеседования, сопровождая наглядными примерами.
Оценка «хорошо» выставляется студенту, если он в ходе собеседования ответил на вопрос по теме собеседования, при этом есть неуверенность с практическими примерами.
Оценка «удовлетворительно» выставляется студенту, если он ходе собеседования ответил неуверенно на вопросы по теме собеседования, не смог привести практические примеры.
Оценка «неудовлетворительно» выставляется студенту, если он не ответил на вопрос по теме собеседования.

2. Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения данного оценочного мероприятия включает в себя устные ответы студентов на вопросы собеседования.

Предлагаемые студенту вопросы позволяют проверить компетенции ОПК-3, ОПК-7, ОПК-9 и ПК-1.

Каждому студенту предлагается ответить на два вопроса базового уровня и один вопрос повышенного уровня.

Перед собеседованием студенту предоставляется право пользования лекциями, и методическими материалами к самостоятельной работе.

При оценивании ответов студента учитываются:
- полнота и последовательность формулировок;

- умение приводить конкретные примеры по теме вопроса.

Составитель _____ Н.И. Битюцкая
(подпись)

«____»_____20 г.