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

УТВЕРЖДАЮ
Директор НТИ (филиал) СКФУ
Ефанов А.В.
Ф.И.О.
«____» __ 2022 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине
Персональная кибербезопасность

Направление подготовки	09.03.02 Информационные системы и технологии
Направленность (профиль)	Информационные системы и технологии в бизнесе
Форма обучения	очная
Год начала обучения	2022
Реализуется в 1 семестре	

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине «Персональная кибербезопасность». Текущий контроль успеваемости и промежуточная аттестация по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля успеваемости и промежуточной аттестации 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 «Персональная кибербезопасность» и в соответствии с образовательной программой высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии.

3. Разработчик: Кочеров Юрий Николаевич, доцент базовой кафедры Регионального индустриального парка, кандидат технических наук

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:
Мельникова Е.Н. – председатель УМК НТИ (филиал) СКФУ

Члены комиссии:
А.И. Колдаев, и.о. зав. кафедрой информационных систем, электропривода и автоматики
Э.Е. Тихонов, доцент базовой кафедры территории опережающего социально-экономического развития

Представитель организации-работодателя:
Горшков М. Г., директор ООО «Арнест-информационные технологии"

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 09.03.02 Информационные системы и технологии и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Персональная кибербезопасность».

05 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
ИД-1 ПК-4 ИД-2 ПК-4 ИД-3 ПК-4	1-6	Собеседование	Текущий	Устный	Вопросы для собеседования
ИД-1 ПК-4 ИД-2 ПК-4 ИД-3 ПК-4	1-6	Тестирование	Текущий	Устный	Паспорт фонда тестовых заданий

2. 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
ПК-4 Способен разработать архитектуру ИС				
ИД-1 ПК-4 ИД-2 ПК-4	Не удовлетворительно понимает история развития криптографии; основные понятия и определения информационной безопасности; Не удовлетворительно осуществляет методы защиты информации с применением	Слабо понимает история развития криптографии; основные понятия и определения информационной безопасности; Слабо осуществляет методы защиты информации с применением симметричных алгоритмов шифрования;	Понимает история развития криптографии; основные понятия и определения информационной безопасности; Осуществляет методы защиты информации с применением симметричных алгоритмов шифрования; Применяет	На высоком уровне понимает история развития криптографии; основные понятия и определения информационной безопасности; На высоком уровне осуществляет методы защиты информации с применением симметричных

	симметричных алгоритмов шифрования; Не удовлетворительно применяет приемов облачного программирования; методы защиты информации с применением асимметричных алгоритмов шифрования	Слабо применяет приемов облачного программирования; методы защиты информации с применением асимметричных алгоритмов шифрования	приемов облачного программирования; методы защиты информации с применением асимметричных алгоритмов шифрования	алгоритмов шифрования; На высоком уровне применяет приемов облачного программирования; методы защиты информации с применением асимметричных алгоритмов шифрования
ИД-3 ПК-4	Не удовлетворительно понимает классификация угроз информационной безопасности; Не удовлетворительно анализирует методы защиты информации с применением методов основанных на разделении данных; Не удовлетворительно применяет математические модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации	Слабо понимает классификация угроз информационной безопасности; Слабо анализирует методы защиты информации с применением методов основанных на разделении данных; Слабо применяет математические модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации	Хорошо понимает классификация угроз информационной безопасности; Хорошо анализирует методы защиты информации с применением методов основанных на разделении данных; Хорошо применяет математические модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации	Понимает классификация угроз информационной безопасности; Анализирует методы защиты информации с применением методов основанных на разделении данных; Применяет математические модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации

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 семестр			
1	Собеседование по темам 1-2, Защита практических работ	8	25
2	Собеседование по теме 3-5, Защита лабораторных работ	16	30
	Итого за 1 семестр:		55
	Итого:		55

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***
Неудвлетворительный	***0***

Промежуточная аттестация

Промежуточная аттестация в форме **зачета или зачета с оценкой**

Процедура зачета (зачета с оценкой) 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 имеет от 33 до 60 баллов, ему ставится отметка «зачтено». Обучающемуся, имеющему по итогам семестра 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 ($S_{зач}$)**
$50 \le R_{сем} \le 60$	**40**
$39 \le R_{сем} < 50$	**35**
$33 \le R_{сем} < 39$	**27**
$R_{сем} < 33$	**0**

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

Вопросы для собеседования

Тема 1. История развития криптографии

1) Криптография древнего периода.
2) Криптография в средние века.

Тема 2. Основные понятия и определения информационной безопасности

1) В чем отличия Информации открытого и ограниченного доступа
2) Какая информация относится к конфиденциальной

Тема 3. Классификация угроз информационной безопасности

1) Источник угрозы – это…
2) Угроза (действие) – это…
3) Фактор (уязвимость) – это…
4) Последствия (атака) – это…

Тема 4. Методы защиты информации с применением симметричных алгоритмов шифрования

1) Методы защиты информации с применением симметричных алгоритмов шифрования
2) Виды алгоритмов симметричного шифрования
3) Достоинства и недостатки симметричного шифрования
4) Чем шифрование отличается от кодирования?
5) Должен ли быть секретным алгоритм шифрования?
6) Должен ли быть секретным ключ шифра при симметричном шифровании?
7) Кто может знать алгоритм шифрования?
8) Кто должен знать ключ шифра?
9) Опишите как получается матрица Виженера.
10) Опишите методику шифрования текста шифром Виженера.
11) Опишите методику шифрования с закрытым ключом.
12) Опишите логическую операцию XOR.

Тема 5. Методы защиты информации с применением асимметричных алгоритмов шифрования

1) Основные понятия и определения асимметричного шифрования
2) Принцип действия асимметричного шифрования
3) Применение асимметричных алгоритмов
4) В чем заключается алгоритм RSA?
5) Для чего и почему используют комбинированные криптоалгоритмы?

Тема 6. Методы защиты информации с применением методов основанных на разделении данных

1) Основные понятия и определения разделения данных
2) Методы разделения данных основанные на геометрических законах и численные примеры их реализации
3) Поясните концепцию разбиения данных. Приведите пример.
4) Поясните концепцию порогового разделения данных. Приведите пример.
5) Поясните преимущества использование системы остаточных классов для разделения секрета.
6) Каким образом информация из системы остаточных классов переводится в десятичную систему счисления с применением обобщенной полиадической системы счисления.

Повышенный уровень

Тема 1 История развития криптографии

1) Криптография в эпоху Возрождения (XIV-XVI вв.)
2) Криптография XVII-XX веков.
3) Современная криптография

Тема 2. Основные понятия и определения информационной безопасности

1) Что понимается под термином «Пользователь информации»
2) Что понимают под качеством информации

Тема 3. Классификация угроз информационной безопасности

1) Ущерб как категория классификации угроз
2) Классификация угроз информационной безопасност
3) Классификация источников угроз
4) Техногенные источники угроз
5) Ранжирование источников угроз

Тема 4. Методы защиты информации с применением симметричных алгоритмов шифрования

1) Область применения симметричного шифрования
2) Шифры перестановки. Анализ шифра простой перестановки.
3) Криптоанализ перестановок. Метод диграмм
4) Шифры замены. Анализ шифра замены.
5) Что делать, если размер ключа меньше размера текста?
6) В чем заключается идея шифра простой замены?
7) Алфавиты открытого текста и шифртекста совпадают или отличаются?
8) Как соотносятся частоты появления открытого текста и шифротекста?
9) Сколько уникальных вариантов ключа можно получить для заданного размера блока?
10) Опишите методику нахождения длинны ключевого слова.
11) Опишите методику нахождения ключевого слова если известна его длинна.

12)Механизм работы шифрования на основе XOR.

13)Насколько надежен рассмотренный алгоритм шифрования на основе XOR?

Тема 5. Методы защиты информации с применением асимметричных алгоритмов шифрования

1) Асимметричные алгоритмы
2) Надежность асимметричного шифрования
3) В чем заключаются достоинства и недостатки асимметричных алгоритмов?
4) В чем заключаются достоинства и недостатки симметричных алгоритмов?

Тема 6. Методы защиты информации с применением методов основанных на разделении данных

1) Основные понятия Системы остаточных классов
2) Методы разделения данных основанные на системе остаточных классов примеры их реализации
3) Расскажите принцип порогового разделения данных с применением схемы Шамира.
4) 4) Расскажите принцип порогового разделения данных с применением схемы Блэкли.
5) Расскажите принцип порогового разделения данных с применением схемы Миньотта.
6) Расскажите принцип порогового разделения данных с применением схемы Асмута-Блума.

Компетентностно-ориентированные задания

1) Используя таблицу частот, биграмм русского языка представленную в методических указаниях найдите какие пары букв встречаются чаще всего.
2) Используя ключевое слово «МАЙ» и таблицу Виженера представленную в методических указаниях расшифруйте следующий текст: «ЫРСОЕЫЛМСЬ».
3) Дано сообщение, представленное в десятичной системе счисления «1410» и ключ «1210» зашифруйте и расшифруйте его.
4) Для сообщения длинной 4 Bit выберите и обоснуйте простые числа для вычисления функции Эйлера и вычислите ее.
5) Для восстановления данных в схеме Блэкли необходимо решить систему уравнений $\begin{cases} 6x_1 + 5x_2 + 6x_3 = 340 \\ 9x_1 + 3x_2 + 1x_3 = 461 \\ 5x_1 + 1x_2 + 6x_3 = 282 \end{cases}$. Восстановите разделенные данные любым доступным Вам способом, представленные в системе.

6) Выберите и обоснуйте ряд чисел для представления числа «15» в системе остаточных классов

1. Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если он

На высоком уровне понимает история развития криптографии; основные понятия и определения информационной безопасности;

На высоком уровне осуществляет методы защиты информации с применением симметричных алгоритмов шифрования;

На высоком уровне применяет приемов облачного программирования; методы защиты информации с применением асимметричных алгоритмов шифрования

Понимает классификация угроз информационной безопасности;

Анализирует методы защиты информации с применением методов основанных на разделении данных;

Применяет математические модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации

Оценка «хорошо» выставляется студенту, если он

Понимает история развития криптографии; основные понятия и определения информационной безопасности;

Осуществляет методы защиты информации с применением симметричных алгоритмов шифрования;

Применяет приемов облачного программирования; методы защиты информации с применением асимметричных алгоритмов шифрования

Хорошо понимает классификация угроз информационной безопасности;

Хорошо анализирует методы защиты информации с применением методов основанных на разделении данных;

Хорошо применяет математические модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации

Оценка «удовлетворительно» выставляется студенту, если он

Слабо понимает история развития криптографии; основные понятия и определения информационной безопасности;

Слабо осуществляет методы защиты информации с применением симметричных алгоритмов шифрования;

Слабо применяет приемов облачного программирования; методы защиты информации с применением асимметричных алгоритмов шифрования

Слабо понимает классификация угроз информационной безопасности;

Слабо анализирует методы защиты информации с применением методов основанных на разделении данных;

Слабо применяет математические модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации

Оценка «неудовлетворительно» выставляется студенту, если он

Не удовлетворительно понимает история развития криптографии; основные понятия и определения информационной безопасности;

Не удовлетворительно осуществляет методы защиты информации с применением симметричных алгоритмов шифрования;

Не удовлетворительно применяет приемов облачного программирования; методы защиты информации с применением асимметричных алгоритмов шифрования

Не удовлетворительно понимает классификация угроз информационной безопасности;

Не удовлетворительно анализирует методы защиты информации с применением методов основанных на разделении данных;

Не удовлетворительно применяет математические модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации

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: собеседование

Предлагаемые студенту вопросы позволяют проверить ИД-1 $_{ПК-4}$, ИД-2 $_{ПК-4}$, ИД-3 $_{ПК-4}$ компетенции.

Для подготовки к данному оценочному мероприятию необходимо 10 минут.

При подготовке к ответу студенту предоставляется право пользования отчетами о выполненных лабораторных работах.

При проверке задания, оцениваются последовательность и логика ответа

Оценочный лист

№ п/п	ФИО студента	Критерий оценивания			Итого
		правильность ответа	полнота раскрытия вопроса	умение аргументировать свой ответ	
1					
2					
…					

Паспорт фонда тестовых заданий по дисциплине Персональная кибербезопасность

ПК-2 Способен выполнять работы по созданию (модификации) и сопровождению ИС, автоматизирующих задач организационного управления и бизнеспроцессов

№ п/п	Тест	Ключ
1.	Сведения в военной области относятся к: 1. коммерческой тайне; 2. персональным данным; 3. государственной тайне.	3. государственной тайне
2.	Персональные данные гражданина РФ относятся к… 1. государственной тайне; 2. коммерческой тайне; 3. общедоступной информации; 4. конфиденциальной информации.	4. конфиденциальной информации

3.	Как называется любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу? 1. личные данные; 2. индивидуальные данные; 3. субъективные данные; 4. персональные данные.	4. персональные данные.
4.	Информация о состоянии окружающей среды относится к… 1. государственной тайне; 2. коммерческой тайне; 3. конфиденциальной информации; 4. общедоступным сведениям.	4. общедоступным сведениям.
5.	Как называется информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации? 1. субъект защиты; 2. автоматизированная система; 3. объект информатизации; 4. объект защиты.	4. объект защиты.
6.	Какая логическая цепочка является корректной? 1. Источник угрозы - уязвимость -атака- угроза; 2. Источник угрозы - угроза - уязвимость -атака; 3. Угроза-уязвимость-источник угрозы-атака; 4. Источник угрозы - уязвимость-угроза-атака.	4. Источник угрозы - уязвимость-угроза-атака.
7.	Как называется слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами? 1. источник угрозы; 2. атака; 3. ошибка; 4. уязвимость.	4. уязвимость.
8.	Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации? 1. уязвимость; 2. источник угрозы; 3. атака; 4. угроза.	4. угроза.
9.	Как называется попытка реализации угрозы? 1. нападение; 2. уязвимость; 3. информационная война; 4. атака.	4. атака.
10.	К какой категории по степени воздействия на объект защиты относятся угрозы, не нарушающие состав и нормальную работу объекта защиты? 1. естественные; 2. искусственные; 3. активные;	4. пассивные.

	4. пассивные.	
11.	К какой категории по степени воздействия на объект защиты относятся угрозы, нарушающие состав и нормальную работу объекта защиты? 1. естественные; 2. искусственные; 3. пассивные; 4. активные.	4. активные.
12.	Потенциальная возможность заражения информационной системы вирусом является примером… 1. угрозы нарушения доступности; 2. угрозы нарушения конфиденциальности; 3. угрозы нарушения целостности.	3. угрозы нарушения целостности.
13.	Потенциальная возможность повреждения оборудования из-за короткого замыкания является примером… 1. угрозы нарушения целостности; 2. угрозы нарушения конфиденциальности; 3. угрозы нарушения доступности.	3. угрозы нарушения доступности.
14.	Как называется доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС)? 1. нелегальный доступ; 2. технический канал утечки; 3. неправомерный доступ; 4. несанкционированный доступ;	4. несанкционированный доступ;
15.	Какой вид атаки направлен на получение конфиденциальной информации путем прослушивания сети? 1. сканирование сети; 2. навязывание ложного маршрута; 3. внедрение ложного объекта; 4. анализ сетевого трафика.	4. анализ сетевого трафика.
16.	Целью какой атаки является нарушение доступности информации для законных субъектов информационного обмена? 1. анализ сетевого трафика; 2. сканирование сети; 3. внедрение ложного объекта; 4. отказ в обслуживании.	4. отказ в обслуживании.
17.	Как называется воздействие на защищаемую информацию с помощью вредоносных программ? 1. программно-аналитическое воздействие; 2. программно-аппаратное воздействие; 3. технически-математическое воздействие; 4. программно-математическое воздействие.	4. программно-математическое воздействие.
18.	Как называется программа, которая, являясь частью другой программы с известными пользователю функциями, способна втайне от него выполнять	4. троянский конь.

	некоторые дополнительные действия с целью причинения ему определенного ущерба? 1. вирус; 2. сетевой червь; 3. макровирус; 4. троянский конь.	
19.	Как называется вредоносная программа, распространяющаяся по сетевым каналам, способная к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий? 1. троянский конь; 2. вирус; 3. макровирус; 4. сетевой червь.	4. сетевой червь;
20.	По среде обитания вирусы подразделяются на: 1. файловые, загрузочные, аппаратные; 2. файловые, загрузочные; 3. файловые, сетевые, аппаратные; 4. файловые, загрузочные, сетевые.	4. файловые, загрузочные, сетевые;
21.	Вирус, написанный на макроязыке, встроенном в Word, называется… 1. полиморфным; 2. метаморфным; 3. файловым; 4. макровирусом.	4. макровирусом.
22.	В соответствии с ФЗ №149 "Об информации, информационных технологиях и о защите информации" информация разделяется на следующие категории: 1. общедоступная и конфиденциальная; 2. ограниченного доступа и государственная тайна; 3. конфиденциальная информация и государственная тайна; 4. общедоступная и ограниченного доступа.	4. общедоступная и ограниченного доступа.
23.	Выделите верное определение термина "информация". Информация - это… 1. сведения (сообщения, данные) в зависимости от формы их представления; 2. сведения (сообщения, данные) независимо от формы их представления, которые может воспринять человек; 3. сведения (сообщения, данные), доступ к которым ограничен; 4. сведения (сообщения, данные) независимо от формы их представления.	4. сведения (сообщения, данные) независимо от формы их представления.
24.	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов это… 1. информационная система;	4. информационная технология.

	2. автоматизированная система; 3. информационно - телекоммуникационная сеть; 4. информационная технология.	
25.	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств это… 1. информационная технология; 2. автоматизированная система; 3. информационно - телекоммуникационная сеть; 4. информационная система.	4. информационная система.
26.	Какая буква русского языка имеет самую максимальную частотность (результат ы нижнем регистре)	о
27.	Дано сообщение 10001_2 и ключ 00111_2 в двоичноq системе счисления. Каков будет результат если применить алгоритм шифрования XOR	10110
28.	Даны 2 простых числа 5 и 7 вычислите значение функции Эйлера от числа n, где n=5*7=35	24
29.	Дан ряд простых чисел 2, 3, 5. В ответ впишите результат целочисленного деления числа 7 на указанный ряд. (В ответе числа указать подряд без пробелов и знаков препинания)	112
30.	Для таблицы Виженера русского языка с какой букв начнется вторая строка (ответ написать с нижнего регистра)	б

1. Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если он

На высоком уровне понимает история развития криптографии; основные понятия и определения информационной безопасности;

На высоком уровне осуществляет методы защиты информации с применением симметричных алгоритмов шифрования;

На высоком уровне применяет приемов облачного программирования; методы защиты информации с применением асимметричных алгоритмов шифрования

Понимает классификация угроз информационной безопасности;

Анализирует методы защиты информации с применением методов основанных на разделении данных;

Применяет математические модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации

Оценка «хорошо» выставляется студенту, если он

Понимает история развития криптографии; основные понятия и определения информационной безопасности;

Осуществляет методы защиты информации с применением симметричных алгоритмов шифрования;

Применяет приемов облачного программирования; методы защиты информации с применением асимметричных алгоритмов шифрования

Хорошо понимает классификация угроз информационной безопасности;

Хорошо анализирует методы защиты информации с применением методов основанных на разделении данных;

Хорошо применяет математические модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации

Оценка «удовлетворительно» выставляется студенту, если он

Слабо понимает история развития криптографии; основные понятия и определения информационной безопасности;

Слабо осуществляет методы защиты информации с применением симметричных алгоритмов шифрования;

Слабо применяет приемов облачного программирования; методы защиты информации с применением асимметричных алгоритмов шифрования

Слабо понимает классификация угроз информационной безопасности;

Слабо анализирует методы защиты информации с применением методов основанных на разделении данных;

Слабо применяет математические модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации

Оценка «неудовлетворительно» выставляется студенту, если он

Не удовлетворительно понимает история развития криптографии; основные понятия и определения информационной безопасности;

Не удовлетворительно осуществляет методы защиты информации с применением симметричных алгоритмов шифрования;

Не удовлетворительно применяет приемов облачного программирования; методы защиты информации с применением асимметричных алгоритмов шифрования

Не удовлетворительно понимает классификация угроз информационной безопасности;

Не удовлетворительно анализирует методы защиты информации с применением методов основанных на разделении данных;

Не удовлетворительно применяет математические модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации