МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет прикладной математики и информатики
Кафедра прикладной математики и информатики по областям

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
041CD9B1001CAF77894D606F5F479EB1E9
Владелец: Сахарчук Елена Сергеевна
Действителен: с 26.09.2022 до 26.09.2023

«Утверждаю»
Зав. кафедрой
Петрунина Е.В.
«26» августа 2020

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Криптография

образовательная программа направления подготовки
01.03.02 "Прикладная математика и информатика"
Б1.В.ДВ.05.01 «Дисциплины (модули)», часть, формируемая участниками образовательных отношений, дисциплины (модули) по выбору

Профиль подготовки
Вычислительная математика и информационные технологии

Квалификация (степень) выпускника
Бакалавр

Форма обучения: очная

Курс 4 семестр 8

Москва
2020

Составитель / составители: доцент кафедры прикладной математики и информатики по областям


подпись

Белоглазов А.А. «24»августа 2020
Ф.И.О. Дата

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры прикладной математики и информатики по областям протокол № 1 от «28» августа 2019

Зав. кафедрой  Петрунина Е.В. «28»августа 2020
Подпись Ф.И.О. Дата

Дополнения и изменения, внесенные в фонд оценочных средств, утверждены на заседании кафедры

_____,

протокол №_____от «____»_____20___г.

Заведующий кафедрой_____/ Ф.И.О/

Дополнения и изменения, внесенные в фонд оценочных средств, утверждены на заседании кафедры

_____,

протокол №_____от «____»_____20___г.

Заведующий кафедрой_____/ Ф.И.О/

Дополнения и изменения, внесенные в фонд оценочных средств, утверждены на заседании кафедры

_____,

протокол №_____от «____»_____20___г.

Заведующий кафедрой_____/ Ф.И.О/

СОДЕРЖАНИЕ

1 ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ..... 4

2 ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ..... 5

3 ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ НА РАЗЛИЧНЫХ ЭТАПАХ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ..... 6

3.1 Критерии оценки аудиторных контрольных и самостоятельных работ: 6

3.2 Критерии оценки тестирования 7

3.3 Критерии оценки устного опроса 7

3.4 Критерии оценки экзамена 8

4 МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ 17

4.1 Задания в форме устного опроса:..... 17

4.2 Задания в форме тестирования..... **Ошибка! Закладка не определена.**

4.3 Материалы для проведения текущего контроля и промежуточной аттестации..... **Ошибка! Закладка не определена.**

4.4 Задания в форме аудиторных контрольных и самостоятельных работ 17

4.5 Задания в форме устного опроса:..... 18

4.6 Задания в форме тестирования..... **Ошибка! Закладка не определена.**

5 МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ..... 17

5.1 Вопросы к экзамену..... 17

1 ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Криптография»

Таблица 1.

№ п/п	Контролируемые разделы (темы), дисциплины[1]	Коды компетенций	Оценочные средства - наименование	
			текущий контроль	промежуточная аттестация
1	История и основные направления развития современной защитой информации	ОПК-1; ОПК-2; ОПК-3; ОПК-4	Устный Опрос	*вопросы к экзамену*
2.	Криптография с открытым ключом	ОПК-1; ОПК-2; ОПК-3; ОПК-4	Устный Опрос, контрольная работа	*вопросы к экзамену*
3.	Криптографические протоколы	ОПК-1; ОПК-2; ОПК-3; ОПК-4	Устный Опрос, тестирование	*вопросы к экзамену*
4	Шифры с секретным ключом	ОПК-1; ОПК-2; ОПК-3; ОПК-4	Устный Опрос, тестирование, контрольная работа	*вопросы к экзамену/экзамен*

Таблица 2.

Перечень компетенций:

Код компетенции	**Наименование результата обучения**
ОПК-1	способностью использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с прикладной математикой и информатикой;
ОПК-2	способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии;
ОПК-3	способностью к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям.
ОПК-4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

[1]Наименование раздела (темы) берется из рабочей программы дисциплины.

2 ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

Таблица 3.

№	Наименование оценочного средства	Характеристика оценочного средства	Представление оценочного средства в ФОС
1	Устный опрос	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
2	Решение аудиторных контрольных и самостоятельных работ	Различают задачи (задания): а) репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины; б) реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей; в) творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.	Комплект разноуровневых задач (заданий), контрольная работа
3	Тест	Средство, позволяющее оценить уровень знаний обучающегося путем выбора им одного из нескольких вариантов ответов на поставленный вопрос. Возможно использование тестовых вопросов, предусматривающих ввод обучающимся короткого и однозначного ответа на поставленный вопрос.	Тестовые задания
4	Экзамен		Вопросы к экзамену

3 ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ НА РАЗЛИЧНЫХ ЭТАПАХ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

При проведении текущего контроля успеваемости студентов по учебной дисциплине Б1.Б.21 «Криптография» используются следующие критерии оценок:

Критерии оценки аудиторных контрольных и самостоятельных работ:

Все запланированные аудиторные контрольные, самостоятельные работы и тесты по дисциплине обязательны для выполнения.

Оценку «отлично» получают ответы, в которых делаются самостоятельные выводы, дается аргументированная критика и самостоятельный анализ фактического материала на основе глубоких знаний литературы по данной теме;

Оценка "хорошо" ставится студенту, проявившему полное и знание учебного материала, но нет должной степени самостоятельности;

Оценка "удовлетворительно" ставится студенту, проявившему знания основного учебного материала в объеме, необходимом для последующего обучения и предстоящей практической деятельности, но в основном обладающему необходимыми знаниями и умениями для их устранения при корректировке со стороны преподавателя.

Оценка "неудовлетворительно" ставится студенту, обнаружившему существенные пробелы в знании основного учебного материала, допустившему принципиальные ошибки при применении теоретических знаний, которые не позволяют ему продолжить обучение или приступить к практической деятельности без дополнительной подготовки по данной дисциплине.

Процент результативности	Оценка уровня подготовки	
	балл (отметка)	вербальный аналог
90 ÷ 100	5	отлично
80 ÷ 89	4	хорошо
70 ÷ 79	3	удовлетворительно
менее 70	2	неудовлетворительно

Критерии оценки устного опроса

Устный опрос используется для текущего контроля успеваемости обучающихся по дисциплине в качестве проверки результатов освоения терминологии.

Каждому студенту выдается свой собственный, узко сформулированный вопрос.

Ответ должен быть четким и кратким, содержащим все основные характеристики описываемого понятия, института, категории.

Описание критериев и шкалы оценивания устного опроса

Критерий оценивания	Оценка
Выставляется обучающемуся, который подготовил ответ на предложенный вопрос, активно участвует в дискуссии, высказывает собственное мнение, представляет наглядный материал	Отлично
Выставляется обучающемуся, который подготовил ответ на предложенный вопрос, но неактивном участии в дискуссии	Хорошо
Выставляется обучающемуся, который частично подготовил ответ на предложенный вопрос, неактивно участвовал в дискуссии	Удовлетворительно
Выставляется обучающемуся в случае его неготовности к занятию	Неудовлетворительно

Критерии оценки тестирования

Тест представляет собой контрольное мероприятие по учебному материалу каждой темы (раздела) дисциплины, состоящее в выполнении обучающимся системы стандартизированных заданий, которая позволяет автоматизировать процедуру измерения уровня знаний и умений обучающегося.

Тестирование является средством текущего контроля успеваемости обучающихся по дисциплине и может включать в себя следующие типы заданий: задание с единственным выбором ответа из предложенных вариантов, задание на определение верных и неверных суждений; задание с множественным выбором ответов.

Описание критериев и шкалы оценивания тестирования

Критерий оценивания	Оценка
Выставляется обучающемуся при правильных ответах на 80-100% тестов	Отлично
Выставляется обучающемуся при правильных ответах на 60-79% тестов.	Хорошо
Выставляется обучающемуся при правильных ответах на 50-59% тестов.	Удовлетворительно
Выставляется обучающемуся, если правильно даны ответы менее чем на 50% тестов.	Неудовлетворительно

Критерии оценки экзамена

Экзамен представляет собой форму итогового контроля знаний по дисциплине и проводится после изучения всех тем учебной дисциплины. Он проводится в устной форме по билетам.

В ходе ответа на вопросы билета обучающийся должен показать сформированность компетенции (или компетенций) по дисциплине.

Результаты ответа на вопросы билета определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Структура билета состоит из трех вопросов: два теоретических вопроса и одна задача.

На подготовку ответа отводится 30 минут.

Описание критериев и шкалы оценивания экзамена

Показатели	**Максимальная оценка в баллах**
1-й вопрос	30
2-й вопрос	30
Задача	40

0-50 баллов	51-70	71-85	86-100
Неудовлетворительно	Удовлетворительно	Хорошо	Отлично

Для оценки уровня освоения дисциплин, профессиональных модулей (их составляющих) устанавливаются следующее соответствие:
«отлично» - высокий уровень освоения;
«хорошо», «удовлетворительно» - достаточный уровень освоения;
«неудовлетворительно» - низкий уровень освоения.

Таблица 4.

Код компетенции	Уровень освоения компетенции	Показатели достижения компетенции	Критерии оценивания результатов обучения
		Знает	
ОПК-1	Недостаточный уровень Оценка «незачтено», «неудовлетворительно»	ОПК-1 З-1 Знать: основные понятия, факты, концепции, принципы теорий естественных наук, математики и информатики ОПК-1 З-2 Знать: Базовый математический аппарат, связанный с прикладной математикой и информатикой;	Не знает или затрудняется в определении основные понятия, факты, концепции, принципы теорий естественных наук, математики и информатики; Имеет фрагментарное представление о базовом математическом аппарате связанным с прикладной математикой и информатикой;
	Базовый уровень Оценка, «зачтено», «удовлетворительно»		Имеет представление о содержании отдельных естественнонаучных дисциплин, знает основные понятия, факты, концепции, принципы теорий естественных наук, математики и информатики, но допускает неточности в формулировках Имеет представление о базовом математическом аппарате связанным с прикладной математикой и информатикой, но допускает неточности в формулировках
	Средний уровень Оценка «зачтено», «хорошо»		Имеет представление о содержании основных учебных курсов по естественнонаучным дисциплинам, знает основные понятия, факты, концепции, принципы теорий естественных наук, математики и информатики; Хорошо знает и понимает базовый математический аппарат, связанный с прикладной математикой и информатикой.
	Высокий уровень Оценка «зачтено», «отлично»		Имеет четкое, целостное представление о содержании основных естественнонаучных курсов и знает и сможет применять основные понятия, факты, концепции, принципы теорий естественных наук, математики и информатики Знает, понимает и умеет применять базовый математический аппарат, связанный с прикладной математикой и информатикой;
		Умеет	
	Базовый уровень	ОПК-1 У-1 Уметь: выполнять стандартные действия, решать типовые задачи с учетом основных понятий и	Умеет решать типовые задачи из базовых курсов естественнонаучных дисциплин, но допускает недочёты в выкладках. В целом успешное, но не систематическое умение понимать и

		общих закономерностей, формулируемых в рамках базовых дисциплин математики, информатики и естественных наук ОПК-1 У-2 Уметь: понимать и применять на практике компьютерные технологии для решения различных задач	применять на практике компьютерные технологии для решения различных
	Средний уровень		Умеет решать комбинированные задачи из базовых курсов естественнонаучных дисциплин В целом успешное, но содержащее отдельные пробелы умение понимать и применять на практике компьютерные технологии для решения различных
	Высокий уровень		Умеет решать задачи повышенной сложности из базовых курсов естественнонаучных дисциплин. Сформированное умение понимать и применять на практике компьютерные технологии для решения различных задач.
		Владеет	
	Базовый уровень	ОПК-1 В-1 Владеть: – навыками работы с учебной литературой по основным естественнонаучным и математическим дисциплинам	Владеет навыками воспроизведения освоенного учебного материала по основным естественнонаучным дисциплинам Владеет недостаточно навыками решения практических задач, базовыми знания естественных наук, математики и информатики, связанными с прикладной математикой и информатикой
	Средний уровень	ОПК-1 В-2 Владеть: навыками решения практических задач, базовыми знания естественных наук, математики и информатики, связанными с математикой и информатикой	Владеет навыками самостоятельного изучения отдельных разделов учебной литературы по основным естественнонаучным дисциплинам и обсуждения освоенного материала Хорошо владеет навыками решения практических задач, базовыми знания естественных наук, математики и информатики, связанными с прикладной математикой и информатикой
	Высокий уровень		Владеет навыками критического анализа учебной информации по основным разделам естественнонаучных дисциплин, формулировки выводов и участия в дискуссии по учебным вопросам. Уверенно владеет навыками решения практических задач, базовыми знания естественных наук, математики и информатики, связанными с прикладной математикой и информатикой.
ОПК-2		Знает	
	Недостаточный уровень Оценка	ОПК-2 З-1 Знать: Современные образовательные и информационные технологии,	Не знает современные образовательные и информационные технологии, информационные системы и ресурсы;

	«незачтено», «неудовлетворительно»	информационные системы и ресурсы	
	Базовый уровень Оценка, «зачтено», «удовлетворительно»		Знает современные информационные технологии, информационные ресурсы;
	Средний уровень Оценка «зачтено», «хорошо»		Знает современные образовательные и информационные технологии, информационные системы и ресурсы;
	Высокий уровень Оценка «зачтено», «отлично»		Знает современные образовательные и информационные технологии, специализированное программное обеспечение, информационные системы и ресурсы;
		Умеет	
	Базовый уровень	ОПК-2 У-1 Уметь: находить, классифицировать и использовать информационные интернет- технологии, базы данных, web- ресурсы, специализированное программное обеспечение для получения новых научных и профессиональных знаний;	Умеет использовать интернет- технологии, базы данных, web- ресурсы, специализированное программное обеспечение для получения новых профессиональных знаний;
	Средний уровень		Умеет находить, классифицировать и использовать информационные базы данных, web- ресурсы, специализированное программное обеспечение для получения новых профессиональных знаний;
	Высокий уровень		Умеет находить, классифицировать и использовать информационные интернет- технологии, базы данных, web- ресурсы, специализированное программное обеспечение для получения новых научных и профессиональных знаний;
		Владеет	
	Базовый уровень	ОПК-2 В-1 Владеть: знаниями в области современных технологий, баз данных, web- ресурсов, специализированного программное обеспечения и т.п. и их практическим применением ОПК-2 В-2 Владеть: навыками работы в информационных современных	Владеет общими представлениями о возможности практического использования знаний в области современных технологий, баз данных, web- ресурсов, специализированного программное обеспечения Владеет частичными навыками поиска информации в информационных современных системах учебного материала по основным дисциплинам.
	Средний уровень		Владеет представлениями и навыками практического использования знаний в области современных технологий, баз

		системах автоматического поиска для получения необходимой информации	данных, web- ресурсов, специализированного программное обеспечения Хорошо владеет навыками поиска информации в информационных современных системах
	Высокий уровень		Свободно владеет представлениями и навыками практического использования знаний в области современных технологий, баз данных, web- ресурсов, специализированного программное обеспечения. Уверенно владеет навыками работы в информационных современных системах поиска информации, свободно находит необходимую научно-техническую информацию.
		Знает	
ОПК-3	Недостаточный уровень Оценка «незачтено», «неудовлетворительно»	ОПК-3 З-1 Знать: принципы работы и программирования в глобальных компьютерных сетях ОПК-3 З-2 Знать: Синтаксис и семантику алгоритмических конструкций языков программирования высокого уровня и СУБД; базовые структуры данных, средства компьютерной графики и основные численные алгоритмы	Не знает или затрудняется в определении принципов работы и программирования в глобальных компьютерных сетях; имеет фрагментарное представление о синтаксисе и семантике алгоритмических конструкций языков программирования высокого уровня и СУБД; базовых структурах данных, средствах компьютерной графики
	Базовый уровень Оценка, «зачтено», «удовлетворительно»		Имеет представление о содержании отдельных принципов работы и программирования в глобальных компьютерных сетях, но допускает неточности в формулировках Имеет представление о синтаксисе и семантике алгоритмических конструкций языков программирования высокого уровня и СУБД; базовых структурах данных, средствах компьютерной графики и основных численных алгоритмах, но допускает неточности в формулировках
	Средний уровень Оценка «зачтено», «хорошо»		Имеет представление о принципах работы и программирования в глобальных компьютерных сетях Хорошо знает и понимает синтаксис и семантику алгоритмических конструкций языков Программирования высокого уровня и СУБД; базовые структуры данных, средства компьютерной графики и основные численные алгоритмы
	Высокий уровень		Имеет четкое, целостное представление о принципах работы и

	Оценка «зачтено», «отлично»		программирования в глобальных компьютерных сетях. Знает, понимает и умеет применять синтаксис и семантику алгоритмических конструкций языков программирования высокого уровня и СУБД; базовые структуры данных, средства компьютерной графики и основные численные алгоритмы
		Умеет	
	Базовый уровень	ОПК-3 У-1 Уметь: разрабатывать математические и информационные модели и алгоритмы для решения прикладных задач	Умеет разрабатывать математические модели и алгоритмы для решения прикладных задач; В целом успешное, но не систематическое умение использовать дополнительные пакеты, средства компьютерной графики и библиотеки при программировании;
	Средний уровень	ОПК-3 У-2 Уметь: использовать дополнительные пакеты, средства компьютерной графики и библиотеки при программировании;	Умеет разрабатывать математические и информационные модели и алгоритмы для решения прикладных задач; В целом успешное, но содержащее отдельные пробелы умение использовать дополнительные пакеты, средства компьютерной графики и библиотеки при программировании;
	Высокий уровень		Умеет разрабатывать математические и информационные модели и алгоритмы для решения прикладных задач повышенной сложности. Сформированное умение использовать дополнительные пакеты, средства компьютерной графики и библиотеки при программировании;
		Владеет	
	Базовый уровень	ОПК-3 В-1 Владеть: навыками работы с системным и прикладным обеспечением для решения задач математического моделирования в своей предметной области, а также современным программным обеспечением, средствами тестирования, верификации и документации ПО; ОПК-3 В-2 Владеть: Навыками	Владеет недостаточно навыками работы с прикладным обеспечением для решения задач математического моделирования в своей предметной области, а также современным программным обеспечением; Владеет недостаточно навыками применения стандартных программных средств на базе математических моделей в конкретных предметных областях; Владеет недостаточно навыками низкоуровневого программирования элементов компьютерной графики, а также навыками разработки, проектирования и тестирования программного обеспечения;

	Средний уровень	применения стандартных программных средств на базе математических моделей в конкретных предметных областях; ОПК-3 В-3 Владеть: Навыками низкоуровневого программирования элементов компьютерной графики, а также навыками разработки, проектирования и тестирования программного обеспечения;	Хорошо владеет навыками работы с системным и прикладным обеспечением для решения задач математического моделирования в своей предметной области, а также современным программным обеспечением, средствами тестирования, верификации и документации ПО; Хорошо владеет навыками применения стандартных программных средств на базе математических моделей в конкретных предметных областях; Хорошо владеет навыками низкоуровневого программирования элементов компьютерной графики, а также навыками разработки, проектирования и тестирования программного обеспечения;
	Высокий уровень		Уверенно владеет навыками работы с системным и прикладным обеспечением для решения задач математического моделирования, а также современным программным обеспечением, средствами тестирования, верификации и документации ПО. Уверенно владеет навыками применения стандартных программных средств на базе математических моделей в конкретных предметных областях; Уверенно владеет навыками низкоуровневого программирования элементов компьютерной графики, а также навыками разработки, проектирования и тестирования программного обеспечения;
		Знает	
ОПК-4	Недостаточный уровень Оценка «незачтено», «неудовлетворительно»	ОПК-4 З-1 Знать: Методы сбора и обработки и хранения информации, а также основные методы формирования научного знания ОПК-4 З-2 Знать: классификацию языков программирования, основные методы разработки программного обеспечения, стандарты оформления	Имеет фрагментарное представление о методах сбора и обработки и хранения информации, а также об основных методах формирования научного знания Не знает классификацию языков программирования, основные методы разработки программного обеспечения, стандарты оформления программной документации и причины нарушения компьютерной безопасности
	Базовый уровень Оценка, «зачтено», «удовлетворительно»		Имеет представление о методах сбора и обработки и хранения информации, а также об основных методах формирования научного знания Имеет представление о классификации языков программирования,

		программной документации и причины нарушения компьютерной безопасности	основные методы разработки программного обеспечения, стандарты оформления программной документации и причины нарушения компьютерной безопасности, но допускает неточности в формулировках
	Средний уровень Оценка «зачтено», «хорошо»		Хорошо знает методы сбора и обработки и хранения информации, а также об основных методах формирования научного знания Имеет представление о классификации языков программирования, основные методы разработки программного обеспечения, стандарты оформления программной документации и причины нарушения компьютерной безопасности
	Высокий уровень Оценка «зачтено», «отлично»		Знает и умеет применять методы сбора и обработки и хранения информации, а также основные методы формирования научного знания Имеет четкое, целостное представление о классификации языков программирования, основные методы разработки программного обеспечения, стандарты оформления программной документации и причины нарушения компьютерной безопасности
		Умеет	
	Базовый уровень	ОПК-4 У-1 Уметь: использовать научные и методические ресурсы сети Интернет для разработки программного обеспечения и программной документации с учетом требований информационной безопасности	В целом успешное, но не систематическое умение использовать научные и методические ресурсы сети Интернет для разработки программного обеспечения и программной документации с учетом требований информационной безопасности Умеет составлять научные обзоры, рефераты и библиографии по тематике научных исследований Умеет использовать только информационные сервисы глобальных телекоммуникаций, базы данных, web-ресурсы
	Средний уровень	ОПК-4 У-2 Уметь: составлять научные обзоры, рефераты и библиографии по тематике научных исследований ОПК-4 У-3 Уметь:	В целом успешное, но содержащее отдельные пробелы умение использовать научные и методические ресурсы сети Интернет для разработки программного обеспечения и программной документации с учетом требований информационной безопасности В целом успешное, но содержащее отдельные пробелы умение

		использовать информационные сервисы глобальных телекоммуникаций, базы данных, web-ресурсы, системное и программное обеспечение	составлять научные обзоры, рефераты и библиографии по тематике научных исследований Умеет использовать информационные сервисы глобальных телекоммуникаций, базы данных, web-ресурсы, системное и программное обеспечение
	Высокий уровень		Сформированное умение использовать научные и методические ресурсы сети Интернет для разработки программного обеспечения и программной документации с учетом требований информационной безопасности Сформированное умение составлять научные обзоры, рефераты и библиографии по тематике научных исследований Умеет находить и использовать информационные сервисы глобальных телекоммуникаций, базы данных, web-ресурсы, системное и программное обеспечение
		Владеет	
	Базовый уровень	ОПК-4 В-1 Владеть: базовыми знаниями по защите информации на рабочем месте, в корпоративных сетях при входе в глобальные сети ОПК-4 В-2 Владеть: навыками системного и объектно- ориентированного программирования для решения стандартных прикладных задач в профессиональной деятельности	Владеет недостаточно базовыми знаниями по защите информации на рабочем месте, в корпоративных сетях при входе в глобальные сети Владеет недостаточно навыками системного и объектно-ориентированного программирования для решения стандартных прикладных задач в профессиональной деятельности
	Средний уровень		Хорошо владеет базовыми знаниями по защите информации на рабочем месте, в корпоративных сетях при входе в глобальные сети Хорошо владеет навыками системного и объектно-ориентированного программирования для решения стандартных прикладных задач в профессиональной деятельности
	Высокий уровень		Уверенно владеет базовыми знаниями по защите информации на рабочем месте, в корпоративных сетях при входе в глобальные сети Уверенно владеет навыками системного и объектно-ориентированного программирования для решения прикладных задач в профессиональной деятельности

4 МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Задания в форме аудиторных контрольных и самостоятельных работ

Контрольные и самостоятельные работы используются для текущего контроля успеваемости обучающихся по дисциплине для проверки умений по освоению методики использования программных средств для решения практических задач, по обоснованию принимаемых проектных решений, по осуществлению постановки и выполнению экспериментов по проверке их корректности и эффективности.

Задания в форме устного опроса

Устный опрос используется для текущего контроля успеваемости обучающихся по дисциплине в качестве проверки результатов освоения терминологии. Каждому студенту выдается свой собственный, узко сформулированный вопрос. Ответ должен быть четким и кратким, содержащим все основные характеристики описываемого понятия, института, категории.

Задания в форме тестирования

Тест представляет собой контрольное мероприятие по учебному материалу каждой темы (раздела) дисциплины, состоящее в выполнении обучающимся системы стандартизированных заданий, которая позволяет автоматизировать процедуру измерения уровня знаний и умений обучающегося.

Тестирование является средством текущего контроля успеваемости обучающихся по дисциплине и может включать в себя следующие типы заданий: задание с единственным выбором ответа из предложенных вариантов, задание на определение верных и неверных суждений; задание с множественным выбором ответов.

В каждом задании необходимо выбрать все правильные ответы.

5 МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Задания в форме аудиторных контрольных и самостоятельных работ

1. Разработать алгоритм шифрования с использованием шифров замены
2. Разработать алгоритм шифрования с использованием шифра перестановки
3. Разработать алгоритм шифрования с использованием квадрата Полибия
4. Разработать алгоритм шифрования с использованием метода прямой замены
5. Разработать алгоритм шифрования с использованием алгоритма моноалфавитной замены
6. Разработать алгоритм шифрования с использованием методов полиалфавитной замены
7. Разработать алгоритм шифрования с использованием (матрицы) Вижинера
8. Разработать алгоритм шифрования с использованием методов перестановки
9. Разработать алгоритм шифрования с использованием маршрутов Гамильтона
10. Разработать алгоритм шифрования с использованием аналитических методов шифрования
11. Разработать алгоритм шифрования с использованием методов шифрования, основанных на использовании матричной алгебры
12. Разработать алгоритм шифрования с использованием аддитивных методов шифрования
13. Разработать алгоритм шифрования с использованием аддитивных методов, в основу которых положено использование генераторов (датчиков) псевдослучайных чисел.

14. Разработать алгоритм шифрования с использованием системы шифрования с открытым ключом

15. Разработать алгоритм шифрования с использованием RSA

Контролируемые компетенции: ОПК-1; ОПК-2; ОПК-3; ОПК-4

Оценка компетенций осуществляется в соответствии с Таблицей 4.

Задания в форме устного опроса

1. Критерии безопасности компьютерных систем
2. Руководящие документы Гостехкомиссии России.
3. Международные стандарты информационной безопасности.
4. Общие принципы построения защищенных систем.
5. Средства разработки и правила их реализации.
6. Фундаментальные проблемы, возникающие при построении защищенных информационных систем.

Контролируемые компетенции: ОПК-1; ОПК-2; ОПК-3; ОПК-4

Оценка компетенций осуществляется в соответствии с Таблицей 4.

Задания в форме тестирования

1. Что такое шифрование?

а) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого

б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств

в) удобная среда для вычисления конечного пользователя

2. Что такое кодирование?

а) преобразование обычного, понятного текста в код

б) преобразование

в) написание программы

3. Для восстановления защитного текста требуется:

а) ключ

б) матрица

в) вектор

4. Сколько лет назад появилось шифрование?

а) четыре тысячи лет назад

б) две тысячи лет назад

в) пять тысяч лет назад

5. Первое известное применение шифра:

а) египетский текст

б) русский

в) нет правильного ответа

6. Секретная информация, которая хранится вWindows:

а) пароли для доступа к сетевым ресурсам

б) пароли для доступа в Интернет

в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

7. Что такое алфавит?

а) конечное множество используемых для кодирования информации знаков

б) буквы текста

в) нет правильного ответа

8. Что такое текст?

а) упорядоченный набор из элементов алфавита

б) конечное множество используемых для кодирования информации знаков

в) все правильные

9. Выберите примеры алфавитов:

а) Z256 – символы, входящие в стандартные коды ASCII и КОИ-8

б) восьмеричный и шестнадцатеричный алфавиты

в) AEE

10. Что такое шифрование?

а) преобразовательный процесс исходного текста в зашифрованный

б) упорядоченный набор из элементов алфавита

в) нет правильного ответа

11. Что такое дешифрование?

а) на основе ключа шифрованный текст преобразуется в исходный

б) пароли для доступа к сетевым ресурсам

в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

12. Что представляет собой криптографическая система?

а) семейство T преобразований открытого текста, члены его семейства индексируются символом k

б) программу

в) систему

13. Что такое пространство ключей k?

а) набор возможных значений ключа

б) длина ключа

в) нет правильного ответа

14. На какие виды подразделяют криптосистемы?

а) симметричные

б) ассиметричные

в) с открытым ключом

15. Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:

а) 1

б) 2

в) 3

16. Количество используемых ключей в системах с открытым ключом:

а) 2

б) 3

в) 1

17. Ключи, используемые в системах с открытым ключом:

а) открытый
б) закрытый
в) нет правильного ответа

18. Выберите то, как связаны ключи друг с другом в системе с открытым ключом:
а) математически
б) логически
в) алгоритмически

19. Что принято называть электронной подписью?
а) присоединяемое к тексту его криптографическое преобразование
б) текст
в) зашифрованный текст

20. Что такое криптостойкость?
а) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа
б) свойство гаммы
в) все ответы верны

21. Выберите то, что относится к показателям криптостойкости:
а) количество всех возможных ключей
б) среднее время, необходимое для криптоанализа+
в) количество символов в ключе

22. Требования, предъявляемые к современным криптографическим системам защиты информации:
а) знание алгоритма шифрования не должно влиять на надежность защиты
б) структурные элементы алгоритма шифрования должны быть неизменными
в) не должно быть простых и легко устанавливаемых зависимостью между ключами последовательно используемыми в процессе шифрования

23. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
а) длина шифрованного текста должна быть равной лине исходного текста+
б) зашифрованное сообщение должно поддаваться чтению только при наличии ключа
в) нет правильного ответа

24. Основными современными методами шифрования являются:
а) алгоритм гаммирования
б) алгоритмы сложных математических преобразований
в) алгоритм перестановки

25. Чем являются символы исходного текста, складывающиеся с символами некой случайной последовательности?
а) алгоритмом гаммирования
б) алгоритмом перестановки
в) алгоритмом аналитических преобразований

26. Чем являются символы оригинального текста, меняющиеся местами по определенному принципу, которые являются секретным ключом?

а) алгоритм перестановки
б) алгоритм подстановки
в) алгоритм гаммирования

27. Самая простая разновидность подстановки:
а) простая замена
б) перестановка
в) простая перестановка

28. Количество последовательностей, из которых состоит расшифровка текста по таблице Вижинера:
а) 3
б) 4
в) 5

29. Таблицы Вижинера, применяемые для повышения стойкости шифрования:
а) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке
б) в качестве ключа используется случайность последовательных чисел+
в) нет правильного ответа

30. Суть метода перестановки:
а) символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов
б) замена алфавита
в) все правильные

31. Цель криптоанализа:
а) Определение стойкости алгоритма
б) Увеличение количества функций замещения в криптографическом алгоритме
в) Уменьшение количества функций подстановок в криптографическом алгоритме
г) Определение использованных перестановок

32. По какой причине произойдет рост частоты применения брутфорс-атак?
а) Возросло используемое в алгоритмах количество перестановок и замещений
б) Алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам
в) Мощность и скорость работы процессоров возросла
г) Длина ключа со временем уменьшилась

33. Не будет являться свойством или характеристикой односторонней функции хэширования:
а) Она преобразует сообщение произвольной длины в значение фиксированной длины
б) Имея значение дайджеста сообщения, невозможно получить само сообщение
в) Получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко
г) Она преобразует сообщение фиксированной длины в значение переменной длины+

34. Выберите то, что указывает на изменение сообщения:
а) Изменился открытый ключ

б) Изменился закрытый ключ
в) Изменился дайджест сообщения
г) Сообщение было правильно зашифровано

35. Алгоритм американского правительства, который предназначен для создания безопасных дайджестов сообщений:
а) Data Encryption Algorithm
б) Digital Signature Standard
в) Secure Hash Algorithm
г) Data Signature Algorithm

36. Выберите то, что лучшеописывает отличия между HMAC и CBC-MAC?
а) HMAC создает дайджест сообщения и применяется для контроля целостности; CBC-MAC используется для шифрования блоков данных с целью обеспечения конфиденциальности
б) HMAC использует симметричный ключ и алгоритм хэширования; CBC-MAC использует первый блок в качестве контрольной суммы
в) HMAC обеспечивает контроль целостности и аутентификацию источника данных; CBC-MAC использует блочный шифр в процессе создания MAC
г) HMAC зашифровывает сообщение на симметричном ключе, а затем передает результат в алгоритм хэширования; CBC-MAC зашифровывает все сообщение целиком

37. Определите преимущество RSA над DSA?
а) Он может обеспечить функциональность цифровой подписи и шифрования
б) Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи
в) Это блочный шифр и он лучше поточного
г) Он использует одноразовые шифровальные блокноты

38. С какой целью многими странами происходит ограничение использования и экспорта криптографических систем?
а) Без ограничений может возникнуть большое число проблем совместимости при попытке использовать различные алгоритмы в различных программах
б) Эти системы могут использоваться некоторыми странами против их местного населения
в) Криминальные элементы могут использовать шифрование, чтобы избежать обнаружения и преследования
г) Законодательство сильно отстает, а создание новых типов шифрования еще больше усиливает эту проблему

39. Выберите то, что используют для создания цифровой подписи:
а) Закрытый ключ получателя
б) Открытый ключ отправителя
в) Закрытый ключ отправителя
г) Открытый ключ получателя

40. Выберите то, что лучше всего описывает цифровую подпись:
а) Это метод переноса собственноручной подписи на электронный документ
б) Это метод шифрования конфиденциальной информации
в) Это метод, обеспечивающий электронную подпись и шифрование
г) Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения

41.Эффективная длина ключа в DES:
а) 56
б) 64
в) 32
г) 16

42. Причина, по которой удостоверяющий центр отзывает сертификат:
а) Если открытый ключ пользователя скомпрометирован
б) Если пользователь переходит на использование модели PEM, которая использует сеть доверия
в) Если закрытый ключ пользователя скомпрометирован
г) Если пользователь переходит работать в другой офис

43. Выберите то, что лучше всего описывает удостоверяющий центр?
а) Организация, которая выпускает закрытые ключи и соответствующие алгоритмы
б) Организация, которая проверяет процессы шифрования
в) Организация, которая проверяет ключи шифрования
г) Организация, которая выпускает сертификаты

44. Расшифруйте аббревиатуру DEA:
а) Data Encoding Algorithm
б) Data Encoding Application
в) Data Encryption Algorithm
г) Digital Encryption Algorithm

45. Разработчик первого алгоритма с открытыми ключами:
а) Ади Шамир
б) Росс Андерсон
в) Брюс Шнайер
г) Мартин Хеллман

46. Процесс, выполняемый после создания сеансового ключа DES:
а) Подписание ключа
б) Передача ключа на хранение третьей стороне (key escrow)
в) Кластеризация ключа
г) Обмен ключом

47. Количество циклов перестановки и замещения, выполняемый DES:
а) 16
б) 32
в) 64
г) 56

48. Выберите правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты:
а) Оно обеспечивает проверку целостности и правильности данных
б) Оно требует внимательного отношения к процессу управления ключами
в) Оно не требует большого количества системных ресурсов
г) Оно требует передачи ключа на хранение третьей стороне (escrowed)

49. Название ситуации, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст:

а) Коллизия
б) Хэширование
в) MAC
г) Кластеризация ключей

50. Определение фактора трудозатрат для алгоритма:а) Время зашифрования и расшифрования открытого текста
б) Время, которое займет взлом шифрования
в)Время, которое занимает выполнение 16 циклов преобразований
г) Время, которое занимает выполнение функций подстановки

51. Основная цельиспользования одностороннего хэширования пароля пользователя:
а) Это снижает требуемый объем дискового пространства для хранения пароля пользователя
б) Это предотвращает ознакомление кого-либо с открытым текстом пароля
в) Это позволяет избежать избыточной обработки, требуемой асимметричным алгоритмом
г) Это предотвращает атаки повтора (replay attack)

52. Алгоритм, основанный на сложности разложения больших чисел на два исходных простых сомножителя:
а) ECC
б) RSA
в)DES
г) Диффи-Хеллман

53. Что является описанием разницы алгоритмов DES и RSA:
а) DES – это симметричный алгоритм, а RSA – асимметричный
б) DES – это асимметричный алгоритм, а RSA – симметричный
в) Они оба являются алгоритмами хэширования, но RSA генерирует 160-битные значения хэша
г) DES генерирует открытый и закрытый ключи, а RSA выполняет шифрование сообщений

54. Алгоритм, использующий симметричный ключ и алгоритм хэширования:
а) HMAC
б) 3DES
в) ISAKMP-OAKLEY
г) RSA

55. Количество способов гаммирования:
а) 2
б) 5
в) 3

56. Показатель стойкости шифрования методом гаммирования:
а) свойство гаммы
б) длина ключа
в) нет правильного ответа

57. То, что применяют в качестве гаммы:
а) любая последовательность случайных символов
б) число
в) все ответы верны

58. Метод, который применяют при шифровании с помощью аналитических преобразований:
а) алгебры матриц
б) матрица
в) факториал

59. То, что применяют в качестве ключа при шифровании с помощью аналитических преобразований:
а) матрица А
б) вектор
в) обратная матрица

60. Способ осуществления дешифрования текста при аналитических преобразованиях:
а) умножение матрицы на вектор
б) деление матрицы на вектор
в) перемножение матриц

1.	а	31.	а
2.	а	32.	в
3.	а	33.	г
4.	а	34.	в
5.	а	35.	в
6.	абв	36.	в
7.	а	37.	а
8.	а	38.	в
9.	аб	39.	в
10.	а	40	г
11.	а	41.	а
12.	а	42.	в
13.	а	43.	г
14.	абв	44.	в
15.	а	45.	г
16.	а	46.	г
17.	аб	47.	а
18.	а	48.	б
19.	а	49.	г
20.	а	50.	б
21.	аб	51.	б
22.	абв	52.	б
23.	Аб	53.	а
24.	абв	54.	а
25.	а	55.	а
26.	а	56.	а
27.	а	57.	а

28.	а	58.	а
29.	аб	59	а
30	а	60	а

Контролируемые компетенции: ОПК-1; ОПК-2; ОПК-3; ОПК-4

Оценка компетенций осуществляется в соответствии с Таблицей 4.

Вопросы к экзамену

1. Основные этапы развития теории защиты информации.
2. Наивная криптография. Шифр Цезаря.
3. Идеальная криптосистема. Шифр Вернама.
4. Система обмена ключами Диффи и Хеллмана.
5. Шифр Шамира.
6. Шифр Эль-Гамаля.
7. Шифр RSA.
8. Электронная цифровая подпись. Схема протокола. Пример построения на основе шифра RSA.
9. Криптосистемы на эллиптических кривых. Основы арифметики на эллиптических кривых. Принцип построения криптосистем на эллиптических кривых.
10. Генераторы псевдо случайных чисел
11. Потоковые шифры. Примеры потоковых шифров.
12. Шифр RC4.
13. Блоковые шифры. Примеры блоковых шифров. Режимы функционирования блоковых шифров.
14. Схема построения потокового шифра на основе блокового шифра.
15. Теорема Шеннона.
16. Расстояние Хемминга. Вес Хэмминга. Код Хэмминнга.
17. Линейные коды. Проверочная матрица. Порождающая матрица.
18. Теорема и связи проверочной и порождающей матриц.
19. Циклические коды.
20. Границы объемов кодов. Граница Хэмминга. Граница Синглтона.

1. Основные этапы развития теории защиты информации.
2. Наивная криптография. Шифр Цезаря.
3. Идеальная криптосистема. Шифр Вернама.
4. Система обмена ключами Диффи и Хеллмана.
5. Шифр Шамира.
6. Шифр Эль-Гамаля.
7. Шифр RSA.
8. Электронная цифровая подпись. Схема протокола. Пример построения на основе шифра RSA.
9. Криптосистемы на эллиптических кривых. Основы арифметики на эллиптических кривых. Принцип построения криптосистем на эллиптических кривых.
10. Генераторы псевдо случайных чисел
11. Потоковые шифры. Примеры потоковых шифров.
12. Шифр RC4.
13. Блоковые шифры. Примеры блоковых шифров. Режимы функционирования блоковых шифров.
14. Схема построения потокового шифра на основе блокового шифра.

15. Теорема Шеннона.
16. Расстояние Хемминга. Вес Хэмминга. Код Хэмминнга.
17. Линейные коды. Проверочная матрица. Порождающая матрица.
18. Теорема и связи проверочной и порождающей матриц.
19. Циклические коды.
20. Границы объемов кодов. Граница Хэмминга. Граница Синглтона.

Контролируемые компетенции: ОПК-1; ОПК-2; ОПК-3; ОПК-4

Оценка компетенций осуществляется в соответствии с Таблицей 4.