МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

"БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

УТВЕРЖДАЮ

Проректор по учебной работе

_____ Е.И.Луковникова

19 _____ 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.07.01 Криптографические методы защиты информации

Закреплена за кафедрой **Информатики, математики и физики**

Учебный план b010302_22_ИПОиЗИ.plx
Направление: 01.03.02 Прикладная математика и информатика

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Виды контроля в семестрах:
Экзамен 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
В том числе инт.	16	16	16	16
В том числе в форме практ.подготовки	32	32	32	32
Итого ауд.	64	64	64	64
Контактная работа	64	64	64	64
Сам. работа	44	44	44	44
Часы на контроль	36	36	36	36
Итого	144	144	144	144

Программу составил(и):
к.т.н., доц., Сташок Ольга Владимировна Сташок

Рабочая программа дисциплины

Криптографические методы защиты информации

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика (приказ Минобрнауки России от 10.01.2018 г. № 9)

составлена на основании учебного плана:

Направление: 01.03.02 Прикладная математика и информатика
утвержденного приказом ректора от 08.02.2022 протокол № 45.

Рабочая программа одобрена на заседании кафедры

Информатики, математики и физики

Протокол от 12 апреля 2022 г. № 9

Срок действия программы: 2022-2026 уч.г.

Зав. кафедрой Горохов Денис Борисович

Председатель МКФ
№ 11 18 апреля 2022 г. Лапшинская СВ

Ответственный за реализацию ОПОП _____ Д.Б. Горохов
(подпись) (ФИО)

Директор библиотеки _____ М.Ф. Сотник
(подпись) (ФИО)

№ регистрации 41
(методический отдел)

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ 2023 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2023 г. № __
Зав. кафедрой Горохов Денис Борисович

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

__ _____ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от __ _____ 2024 г. № __
Зав. кафедрой Горохов Денис Борисович

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

__ _____ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от __ _____ 2025 г. № __
Зав. кафедрой Горохов Денис Борисович

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

__ _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от __ _____ 2026 г. № __
Зав. кафедрой Горохов Денис Борисович

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	ознакомление студентов с основополагающими принципами криптографических методов и алгоритмов защиты информации; с обенностями применения соответствующих криптосистем; изучение принципов защиты информации с помощью криптографических методов и способов; приобретение практических способов применения знаний на практике в области информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.07.01
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Математическое моделирование
2.1.2	Теория вероятностей и математическая статистика
2.1.3	Языки и методы программирования
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Производственная (преддипломная) практика
2.2.2	Выполнение и защита выпускной квалификационной работы
2.2.3	Основы проектирования программных комплексов
2.2.4	Комплексное обеспечение безопасности объекта информатизации

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	
Индикатор 1	УК-2.1 Формулирует в рамках поставленной цели проекта совокупность задач, обеспечивающих ее достижение
Индикатор 2	УК-2.2 Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения
ПК-1 : Способен разрабатывать процедуры документирования, интеграции, преобразования программных модулей, миграции и конвертации данных согласно срокам выполнения поставленных задач	
Индикатор 1	ПК-1.1 Использует выбранную среду программирования для разработки процедур интеграции программных модулей согласно срокам выполнения поставленных задач
Индикатор 2	ПК-1.2 Применяет методы и средства разработки процедур для развертывания программного обеспечения, миграции и преобразования данных

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	способы достижения результатов в рамках поставленной цели; действующие правовые нормы, ресурсы, ограничения при решении задач в предметной области; проводить анализ поставленной цели и формулировать задачи, необходимые для ее достижения; анализировать альтернативные варианты; языки, утилиты и среды программирования, средства пакетного выполнения процедур; методы и средства разработки программного обеспечения, миграции и преобразования данных.
3.2	**Уметь:**
3.2.1	проводить анализ поставленной цели и формулировать задачи, необходимые для ее достижения; выбирать оптимальные способы решения задач предметной области в профессиональной деятельности с учетом действующих правовых норм, ресурсов и ограничений; анализировать альтернативные варианты; внедрять и адаптировать программные модули согласно срокам выполнения поставленных задач; использовать процедуры для развертывания программного обеспечения, миграции и преобразования данных.
3.3	**Владеть:**
3.3.1	методиками разработки цели и задач проекта; приемами планирования решения задач предметной области; навыками проектирования решения конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений; навыками программирования в современных средах; современными языками программирования; современными технологиями разработки, внедрения, адаптации и настройки программного обеспечения и информационных систем.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)								
Код занятия	**Вид занятия**	**Наименование разделов и тем**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Инте ракт.**	**Примечание**

	Раздел	**Раздел 1. Введение в криптографию. Математические операции в криптографии.**						
1.1	Лек	Основные понятия, обозначения и задачи криптографии. Виды нформации, подлежащей шифрованию. Исторические примеры криптосистем.	6	1	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.2	Лаб	Основные принципы крип-тографической защиты информации. Функции шифрования. Односторонние функции.	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.3	Лек	Совершенныешифры.	6	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	2	Лекция - беседа УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.4	Лаб	Симметричные криптосистемы. Метод простой подстановки (замены). Метод перестановки. Метод блочных шифров. Метод гаммирования. Метод шифрования на основе теоремы Эйлера-Ферма. Композиция шифров. Стандарт криптосистемы США DES.	6	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	2	Работа в малых группах. УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.5	Лек	Основные требования к шифрам, к криптографическим системам. Криптостойкость шифров.	6	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	4	Лекция - беседа УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.6	Лаб	Системы защиты с открытым ключом. Криптосистема RSA.	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.7	Ср	Простейшие шифры и их классификация. Стандарткрипто-системы России – ГОСТ 28147-89. Теоретико-числовые алгоритмы и их сложность.	6	1	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.8	Экзамен	Подготовка и сдача экзамена	6	10	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
	Раздел	**Раздел 2. Системы шифрования**						
2.1	Лек	Системы симметричного шифрования	6	6	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
2.2	Лаб	Системы симметричного шифрования	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	2	Работа в малых группах УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
2.3	Ср	Системы симметричного шифрования	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2

2.4	Лек	Системы асимметричного шифрования	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
2.5	Лаб	Системы асимметричного шифрования	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
2.6	Экзамен	Подготовка и сдача экзамена	6	12	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
	Раздел	**Раздел 3. Симметричные криптосистемы**						
3.1	Лек	Основные принципы современных симметричных алгоритмов. Поточные шифры.	6	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
3.2	Лаб	Блочные шифры. Причины ненадежности криптосистем. Принцип Керкхоффа для криптосистемы.	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
3.3	Лек	Генераторы псевдослучайных чисел. Важность подбора параметров.	6	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
3.4	Лаб	Статичный ключ. Эфемерный ключ. Компрометация ключа. Реализация процедуры распределения ключей.	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	2	Работа в малых группах УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
3.5	Ср	Протоколы распределения секретных ключей.	6	20	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
3.6	Экзамен	Подготовка и сдача экзамена	6	6	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
	Раздел	**Раздел 4. Криптографические системы с открытым ключом**						
4.1	Лек	Формула Эйлера. Основные алгоритмы вычисления НОД.	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
4.2	Лаб	Китайская теорема об остатках. Односторонние функции.	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
4.3	Лек	Шифр RSA.	6	1	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
4.4	Лаб	Цифровая подпись. Система электронного голосования.	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
4.5	Ср	Односторонние функции.	6	8	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
4.6	Экзамен	Подготовка и сдача экзамена	6	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
	Раздел	**Раздел 5. Криптографические системы, основанные на физических механизмах защиты информации.**						

5.1	Лек	Криптографические системы, основанные на физических механизмах защиты информации.	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	2	Лекция - беседа УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
5.2	Лаб	Типы, приемы и методы кодирования информации.	6	8	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	2	Работа в малых группах УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
5.3	Лек	Введение в криптографию и криптографические протоколы.	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
5.4	Лаб	Теория криптографических протоколов. Практические криптопротоколы.	6	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
5.5	Ср	Криптографические системы, основанные на физических механизмах защиты информации.Практические криптопротоколы.	6	13	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
5.6	Экзамен	Подготовка и сдача экзамена	6	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии с использованием активных методов обучения (лекция – беседа)

Технология коллективного взаимодействия (работа в малых группах) (самостоятельное изучение обучающимися нового материала посредством сотрудничества в малых группах, дает возможность всем участникам участвовать в работе, практиковать навыки сотрудничества, межличностного общения)

Традиционная (репродуктивная) технология (преподаватель знакомит обучающихся с порядком выполнения задания, наблюдает за выполнением и при необходимости корректирует работу обучающихся)

Технология компьютерного обучения(использование в учебном процессе компьютерных технологий и предоставляемых ими возможностях (электронные библиотеки))

Образовательные технологии с использованием активных методов обучения (лекция – дискуссия)

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

Лекция - беседа №1 (2 часа).
Тема "Совершенные шифры".
Лекция - беседа №2 (4 часа).
Тема "Основные требования к шифрам, к криптографическим системам. Криптостойкость шифров".
Лекция - беседа №3 (2 часа).
Тема "Криптографические системы, основанные на физических механизмах защиты информации".

Лабораторная работа №1 (6 часов).
Тема "Основные принципы криптографической защиты информации. Функции шифрования. Односторонние функции".
Задание: рассмотреть алгоритм шифрования на основе односторонеей функции в соответствии с индщивидуальным вариантом задания.
Вопросы для защиты:
1. Надежность шифра. Имитостойкость и помехоустойчивость шифров.
2.Алгоритмы. Свойства алгоритмов. Требования к алгоритмам.
3.Симметричные криптосистемы (определение, схема, достоинства и недостатки).
Лабораторная работа №2. (4 часа) (2 часа - реализуется в форме работы в малых группах).
Тема "Симметричные криптосистемы. Метод простой подстановки (замены). Метод перестановки. Метод блочных шифров. Метод гаммирования. Метод шифрования на основе теоремы Эйлера-Ферма. Композиция шифров. Стандарт криптосистемы США DES"
Задание: реализовать программно метод простой подстановки и метод перестановки при шифровании в соответствии с индщивидуальным вариантом задания.

Вопросы для защиты:
1.Блочные шифры. Поточные шифры. Атаки на шифры (3 вида)
2.Режимы работы блочного шифра: ECB и CBC (описание, формула и чертеж).
3.Режимы работы блочного шифра: CFB и OFB (описание, формула и чертеж).
4.Шифр Виженера. Шифр Вернама. Шифр DES.
5.ГОСТ 28147-89 (4 режима, схемы, достоинства и недостатки).
Лабораторная работа №3 (2 часа).
Тема "Системы защиты с открытым ключом. Криптосистема RSA"
Задание: рассмотреть алгоритм шифрования RSA в соответствии с индщивидуальным вариантом задания.
Вопросы для защиты:
1.Возможности взлома ас. шифров. Квантовая криптография.
2.Шифр RSA (схема, способы взлома). Обмен ключами Диффи-Хелмана.
3.Шифр Эль Гамаля. Шифр Рабина.
4.Хэш-функции (определение, назначение, условия использования).
Лабораторная работа №4. (2 часа - реализуется в форме работы в малых группах).
Тема "Системы симметричного шифрования"
Задание: рассмотреть алгоритм симметричного шифрования в соответствии с индщивидуальным вариантом задания.
Вопросы для защиты:
1.Алгоритмы. Свойства алгоритмов. Требования к алгоритмам.
2.Симметричные криптосистемы (определение, схема, достоинства и недостатки).
Лабораторная работа №4. (2 часа).
Тема "Системы асимметричного шифрования"
Задание: рассмотреть алгоритм асимметричного шифрования в соответствии с индщивидуальным вариантом задания.
Вопросы для защиты:
1. Асимметричные криптосистемы (определение, схема, свойства, достоинства и недостатки).
2.Возможности взлома ас. шифров. Квантовая криптография.
Лабораторная работа №5. (2 часа).
Тема "Блочные шифры. Причины ненадежности криптосистем. Принцип Керкхоффа для криптосистемы"
Задание: рассмотреть алгоритм блочного шифрования в соответствии с индщивидуальным вариантом задания.
Вопросы для защиты:
1. Криптосистема с секретным ключом. Принцип Керкхоффа. Поточные и блочные шифры.
2. Поточные шифры. Генератор ключевого потока. Свойства генератора ключевого потока. Генератор псевдослучайных чисел, основанный на использовании алгебраических свойств М-последовательностей
3. Статистические тесты генераторов ключевого потока.
Лабораторная работа №6. (2 часа - реализуется в форме работы в малых группах).
Тема "Статичный ключ. Эфемерный ключ. Компрометация ключа. Реализация процедуры распределения ключей"
Задание: рассматреть процедуру распределения ключей в соответствии с индщивидуальным вариантом задания.
Вопросы для защиты:
1. Поточные шифры. Генератор ключевого потока. Свойства генератора ключевого потока.
2. Генератор псевдослучайных чисел, основанный на использовании алгебраических свойств М-последовательностей
3. Статистические тесты генераторов ключевого потока.
4. Статичный ключ. Эфемерный ключ. Распределение ключей.
5. Основные пути решения проблемы распределения ключей. (физические методы, протоколы с секретным ключом, протоколы с открытым ключом, современные физические методы).
Лабораторная работа №7. (2 часа).
Тема "Китайская теорема об остатках. Односторонние функции"
Задание: рассмотреть односторонние функции в алгоритмах шифрования в соответствии с индщивидуальным вариантом задания.
Вопросы для защиты:
1. Сравнение блочных и поточных шифров. Методы организации процедуры исправления ошибок.
Лабораторная работа №8. (2 часа).
Тема "Цифровая подпись. Система электронного голосования"
Задание: рассмотреть специфику алгоритма реализации цифровой подписи в соответствии с индщивидуальным вариантом задания.
Вопросы для защиты:
1.Хэш-функции (определение, назначение, условия использования).
2.Электронная цифровая подпись. Подпись и проверка подписи. Алгоритмы ЭЦП.
3.Подпись RSA. Подпись DSS. подпись ГОСТ Р 34.10-2001.
Лабораторная работа №9. (2 часа - реализуется в форме работы в малых группах).
Тема "Типы, приемы и методы кодирования информации"
Задание: реализовать программно метод кодирования в соответствии с индщивидуальным вариантом задания.
Вопросы для защиты:
1. Разделение секрета. Схема порогового разделения секрета. (T, W) - пороговая схема Шамира.
2. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Барроуза.
3. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Нидхейма-Шредера
4. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Отвэй-Риса.
5. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Цербер.

Лабораторная работа №10. (4 часа).
Тема "Теория криптографических протоколов. Практические криптопротоколы"
Задание: рассмотреть отеорию криптографических протоколов в соответствии с индщивидуальным вариантом задания.
Вопросы для защиты:
1. Функция Эйлера. Мультипликативные обратные по модулю N.
2. Теорема Лагранжа. Малая теорема Ферма. Применение в криптографии.
3. Алгоритм Евклида. Китайская теорема об остатках. Расширенный алгоритм Евклида. Применение в криптографии.
4. Криптосистема с открытым ключом. Криптографическая односторонняя функция.
5. Важнейшие криптографические односторонние функции.
6. Оценка сложности задач. Сложность алгоритма: Полиноминальная, экспоненциальная,субэкспоненциальная Оракул. 7 Сравнительный анализ сложности криптографических алгоритмов (без доказательства).

Тестовое задание для проведения текущего контроля знаний.
1. Конфиденциальность защищаемой информации обеспечивается с помощью...
- электронной подписи
- шифрования
- хэш-функции
2. Способность шифра противостоять попыткам противника по имитации или подмене зашифрованной информации называется
- имитостойкостью.
- криптостойкостью.
- помехозащищенностью.
3. Если криптоаналитик может взломать шифр, но не обладает необходимыми вычислительными ресурсами, то считается, что
- шифр является практически стойким.
- шифр является теоретически стойким.
- шифр является практически имитостойким.
4. Если для шифрования и расшифрования используется один и тот же ключ, то шифр является
- симметричным.
- ассиметричным.
- блочным.
5. Шифры, в которых знание ключа шифрования не позволяет определить ключ расшифрования называются
- поточными.
- симетричными.
- ассиметричными.
6. Шифры, в которых каждый символ открытого текста зашифровывается независимо от других называются
- блочными.
- имитозащищенными.
- поточными.
7. Шифрование информации предназначено для обеспечения
- целостности защищаемой информации
- конфиденциальности защищаемой информации
- доступности защищаемой информации
8. Исходные данные с доступным семантическим содержанием, подлежащие криптографическому преобразованию, называются
- открытый текст
- шифртекст
- имитовставка
9. Параметр шифра, определяющий выбор конкретного варианта преобразования зашифрования или расшифрования из множества преобразований, составляющих шифр, называется…
- алгоритм
- шифр
- ключ
10. Процесс преобразования шифртекста в открытый текст при неизвестном ключе называется…
- дешифрование
- зашифрование
- расшифрование
11.Если за один такт шифрования преобразованию подвергается группа знаков открытого текста, то такой шифр называется
- блочным
- поточным
- ассиметричным
12. На основе сети Фейстеля построен алгоритм шифрования
- AES
- ГОСТ 28147
- RC4
13. Режим использования блочного шифра, при котором блочный шифр может использоваться как поточный называется

- режим простой замены со сцеплением.
- режим гаммирования с обратной связью
- режим простой замены.

14. Режим простой замены заключается в обработке блоков открытого текста независимо от других обработку блоков открытого текста в зависимости от результата зашифрования
- предыдущего блока
- обработку блоков открытого текста в режиме наложения гаммы

15. Шифр называется блочным, если…
- за один такт шифрования преобразованию подвергается группа знаков открытого текста
- за один такт шифрования преобразованию подвергается один знак открытого текста
- группа знаков открытого текста преобразуется за несколько тактов шифрования

16. Если управляющая гамма поточного шифра зависит только от ключа и не зависит от открытого текста и шифротекста, то такой шифр называется
- синхронным.
- самосинхронизирующимся.
- независимым.

17. Достоинством поточных шифров по сравнению с блочными является
- наличие открытого ключа
- высокая стоимость реализации
- высокая скорость работы

18 Недостатком генераторов псевдослучайных последовательностей является
- сложность реализации
- зависимость от параметров окружающей среды
- периодичность последовательности

19. Если управляющая гамма поточного шифра зависит от ключа и от открытого текста и шифротекста, то такой шифр называется
- синхронным.
- самосинхронизирующимся.
- независимым.

20. В алгоритме ГОСТ 34.12-15 размера блока составляет
- 64 бита
- 128 бит, 192 бита и 256 бит
- 64 бита и 128 бит

6.2. Темы письменных работ

не предусмотрено

6.3. Фонд оценочных средств

Экзаменационные вопросы как средство контроля усвоения материала в виде комплекта вопросов по всем темам дисциплины.

Раздел 1. Введение в криптографию. Математические операции в криптографии.

1.1.Определение и основные понятия криптографии. Алгоритм шифрования.

1.2.Периоды развития шифровального дела. Древние шифры (не меньше 5).

1.3.Криптография в России. Основные требования к шифрам.

1.4.Надежность шифра. Имитостойкость и помехоустойчивость шифров.

1.5.Алгоритмы. Свойства алгоритмов. Требования к алгоритмам.

1.6.Симметричные криптосистемы (определение, схема, достоинства и недостатки).

Раздел 2. Системы шифрования.

2.1.Простая перестановка. Одиночная перестановка по ключу. Магический квадрат.

2.2.Блочные шифры. Поточные шифры. Атаки на шифры (3 вида)

2.3.Режимы работы блочного шифра: ECB и CBC (описание, формула и чертеж).

2.4.Режимы работы блочного шифра: CFB и OFB (описание, формула и чертеж).

2.5.Шифр Виженера. Шифр Вернама. Шифр DES.

2.6.ГОСТ 28147-89 (4 режима, схемы, достоинства и недостатки).

Раздел 3. Симметричные криптосистемы.

3.1.Шифр AES. Протоколы: Широкоротой лягушки, Отвэй-Риса и Цербер.

3.2.Асимметричные криптосистемы (определение, схема, свойства, достоинства и недостатки).

3.3.Возможности взлома ас. шифров. Квантовая криптография.

3.4.Шифр RSA (схема, способы взлома). Обмен ключами Диффи-Хелмана.

3.5.Шифр Эль Гамаля. Шифр Рабина.

3.6.Хэш-функции (определение, назначение, условия использования).

3.7.Электронная цифровая подпись. Подпись и проверка подписи. Алгоритмы ЭЦП.

3.8.Подпись RSA. Подпись DSS. подпись ГОСТ Р 34.10-2001.

3.9.Хэш протокол MD4 и MDC.

3.10.Хэш протокол MD5 и RIPEMD.

Раздел 4. Криптографические системы с открытым ключом.

4.1. Криптосистема с секретным ключом. Принцип Керкхоффа. Поточные и блочные шифры.

4.2. Поточные шифры. Генератор ключевого потока. Свойства генератора ключевого потока. Генератор псевдослучайных

чисел, основанный на использовании алгебраических свойств М-последовательностей
4.3. Статистические тесты генераторов ключевого потока.
4.4. Блочные шифры. Алгоритм DES. Перестановки. Раунды. Алгоритм Фейстеля при шифровании и дешифровании.
4.5. Сравнение блочных и поточных шифров. Методы организации процедуры исправления ошибок.
4.6. Статичный ключ. Эфемерный ключ. Распределение ключей. основные пути решения проблемы распределения ключей. (физические методы, Протоколы с секретным ключом,протоколы с открытым ключом, современные физические методы).
4.7. Разделение секрета. Схема порогового разделения секрета. (T, W) - пороговая схема Шамира.
4.8. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Барроуза.
4.9. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Нидхейма-Шредера
4.10. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Отвэй-Риса.
4.11. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Цербер.
4.12. Арифметика остатков. Сравнение по модулю. Решение уравнения ax = b (mod N).
4.13. Функция Эйлера. Мультипликативные обратные по модулю N. Теорема Лагранжа. Малая теорема Ферма. Применение в криптографии.
4.14. Алгоритм Евклида. Китайская теорема об остатках. Расширенный алгоритм Евклида. Применение в криптографии.
Раздел 5. Криптографические системы, основанные на физических механизмах защиты информации.
5.1. Криптосистема с открытым ключом. Криптографическая односторонняя функция.Важнейшие криптографические односторонние функции.
5.2. Оценка сложности задач. Сложность алгоритма: Полиноминальная, экспоненциальная,субэкспоненциальная Оракул. Сравнительный анализ сложности криптографических алгоритмов (без доказательства).
5.3. Алгоритм RSA. Шифрование в RSA. Дешифрование в RSA. Доказательство алгоритма.

6.4. Перечень видов оценочных средств

Лекция - беседа, лабораторные работы, тестовое задание, экзаменационные вопросы.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л1.1	Котов Ю. А.	Криптографические методы защиты информации: шифры: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2016	1	http://biblioclub.ru/index.php?page=book&id=576379
Л1.2	Котов Ю. А.	Криптографические методы защиты информации: стандартные шифры. Шифры с открытым ключом: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2017	1	http://biblioclub.ru/index.php?page=book&id=574782
Л1.3	Кирпичников А. П., Хайбуллина З. М.	Криптографические методы защиты компьютерной информации: учебное пособие	Казань: Казанский научно-исследовательский технологический университет (КНИТУ), 2016	1	http://biblioclub.ru/index.php?page=book&id=560536

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л2.1	Левин М.	Криптография без секретов: Руководство пользователя	Москва: Новый издательский дом, 2005	5	
Л2.2	Осипян В.О., Осипян К.В.	Криптография в упражнениях и задачах: учебное пособие	Москва: Гелиос АРВ, 2004	15	

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Электронная библиотека БрГУ	http://ecat.brstu.ru/catalog

7.3.1 Перечень программного обеспечения

7.3.1.1	Microsoft Windows Professional 7 Russian Upgrade Academic OPEN No Level
7.3.1.2	Microsoft Office 2007 Russian Academic OPEN No Level
7.3.1.3	Visual Studio Community

7.3.1.4	Python IDLE
7.3.2 Перечень информационных справочных систем	
7.3.2.1	«Университетская библиотека online»
7.3.2.2	Электронный каталог библиотеки БрГУ
7.3.2.3	Электронная библиотека БрГУ

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

А1207	Лаборатория технических средств защиты информации	Основное оборудование: - ПК i5-2500/H67/4Gb/500Gb - 11 шт.; -монитор TFT19 Samsung E1920NR- 11 шт.; -комплекс учебно-лабораторного оборудования “Технические средства и методы защиты информации”; -управляемый коммутатор 2 уровня D-Link DES-3028. Дополнительно: - интерактивная доска SMART Board X885ix со встроенным проекторомUX 60 - 1 шт. Учебная мебель: - комплект мебели (посадочных мест /АРМ) - 24 /11 шт. - комплект мебели (посадочных мест/АРМ) для преподавателя - 1/1 шт. ПК i5-2500/H67/4Gb/500Gb; монитор TFT19 Samsung E1920NR.
А1203	Лаборатория параллельных вычислений	Основное оборудование: - ПК i5-2500/H67/4Gb/500Gb- 15 шт.; - монитор TFT19 Samsung E1920NR - 15 шт.; Дополнительно: - доска магнитно-маркерная - 1 шт. - интерактивная доска SMART Board X885ix со встроенным проектором UX 60 - 1 шт. Учебная мебель: - комплект мебели (посадочных мест/АРМ) - 15/15 шт. - комплект мебели (посадочных мест/АРМ) - для преподавателя - 1/ 1 шт. ПК i5-2500/H67/4Gb/500Gb; монитор TFT19 Samsung E1920NR .
2201	читальный зал №1	Комплект мебели (посадочных мест) Стеллажи Комплект мебели (посадочных мест) для библиотекаря Выставочные шкафы ПК i5-2500/H67/4Gb (монитор TFT19 Samsung) (10шт.); принтер HP Laser Jet P2055D (1шт.)

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Обучающийся должен разработать собственный режим равномерного освоения дисциплины. Подготовка студента к предстоящей лекции включает в себя ряд важных познавательно-практических этапов:

- чтение записей, сделанных в процессе слушания и конспектирования предыдущей лекции, вынесение на поля всего, что требуется при дальнейшей работе с конспектом и учебником;
- техническое оформление записей (подчеркивание, выделение главного, выводов, доказательств);
- выполнение практических заданий преподавателя;
- знакомство с материалом предстоящей лекции по учебнику и дополнительной литературе.

Активная работа на лекции, ее конспектирование, продуманная, целенаправленная, систематическая, а главное - добросовестная и глубоко осознанная последующая работа над конспектом - важное условие успешного обучения студентов.

Практические занятия и лабораторные работы позволяют студенту более глубоко разобраться в теоретическом материале и определить сферы его практического применения. Основная цель – развитие самостоятельности студента.

Наиболее продуктивной является самостоятельная работа в библиотеке, где доступны основные и дополнительные печатные и электронные источники.

При выполнении приведенных выше рекомендаций подготовка к экзамену сведется к повторению изученного и совершенствованию навыков применения теоретических положений и различных методов решения к стандартным и нестандартным заданиям.