Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уфимский государственный нефтяной технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические алгоритмы

Направление подготовки (специальность): **09.03.01 Информатика и вычислительная техника**

Направленность: **профиль«Технологии искусственного интеллекта в нефтегазовой отрасли»**

Уровень высшего образования: **бакалавриат**

Форма обучения: **очная;**

Кафедра, обеспечивающая преподавание дисциплины**: Вычислительная техника и инженерная кибернетика (ВТИК);**

Трудоемкость дисциплины: **3 з.е. (108час)**

Уфа

Рабочую программу дисциплины разработал(и):

доцент, канд. физ.-мат. наук Хизбуллина С.Ф.

Рецензент

доцент, канд. физ.-мат. наук Зарипов Д.М.

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры Вычислительная техника и инженерная кибернетика (ВТИК), обеспечивающей преподавание дисциплины 31.08.2022, протокол №1.

И.о. Заведующий кафедрой
Вычислительная техника и инженерная кибернетика (ВТИК) Д.М. Зарипов

СОГЛАСОВАНО

И.о. Заведующий кафедрой ВТИК Д.М. Зарипов

Год приема 2023 г.

Рабочая программа зарегистрирована 19.09.2022 № 1 в УРО и внесена в электронную базу данных

1. Место дисциплины в структуре ОПОП ВО

Дисциплины, предшествующие изучению данной дисциплины (исходя из формирования этапов по компетенциям): Объектно-ориентированное программирование;Статистические и вероятностные методы;Теория чисел и комбинаторика

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее (исходя из формирования этапов по компетенциям): Операционные системы реального времени;Преддипломная практика;Программирование интегральных схем

Блок: Блок 1. Дисциплины (модули);

Обязательная или часть, формируемая участниками образовательных отношений (в том числе элективные дисциплины): Часть, формируемая участниками образовательных отношений;

Форма обучения: очная

Семестр, в котором преподается дисциплина	Трудоемкость дисциплины				Вид промежуточной аттестации
	Зачетные единицы	Часы			
		Общая	В том числе		
			контактная	СРО	
6	3	108	50	58	экзамен;
ИТОГО:	3	108	50	58	

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

№ пп.	Формируемые компетенции	Шифр/ индекс компетенции
1	Способен разрабатывать и тестировать программные компоненты решения задач в системах искусственного интеллекта	ПК-2и-22Г-2
2	Способен разрабатывать и применять методы машинного обучения для решения задач	ПК-4и-22Г-2

В результате освоения дисциплины обучающийся должен:

Шифр компетенции	Индикаторы достижения компетенций	Шифр результата обучения	Результат обучения
ПК-2и-22Г	ПК-2.1. Настраивает программное обеспечение и участвует в разработке программных компонентов систем искусственного интеллекта	З(ПК-2и-22Г)	Знать: основные криптографические стандарты; принципы построения криптографических алгоритмов и использования в информационных

Шифр компетенции	Индикаторы достижения компетенций	Шифр результата обучения	Результат обучения
			системах и системах искусственного интеллекта;
		У(ПК-2и-22Г)	Уметь: решать задачи, связанные с кодированием и защитой информации, настраивать и запускать основные виды криптографического программного обеспечения, направленных на защиту безопасности компьютерной информации;
		В(ПК-2и-22Г)	Владеть: криптографическими методами обеспечения секретности, генерации и распределения ключевой информации, обеспечения целостности и аутентификации; правилами криптографического преобразования для хранения информации в вычислительных системах; вопросами безопасности в Интернет протоколах, системами аппаратной защиты;
ПК-4и-22Г	ПК-4.1. Проводит анализ требований и определяет необходимые классы задач машинного обучения ПК-4.2. Определяет метрики оценки результатов моделирования и критерии качества построенных моделей ПК-4.3. Принимает участие в оценке, выборе и при необходимости разработке	З(ПК-4и-22Г)	Знать: требования к криптографическим системам защиты информации; понятие и виды криптографических атак; виды криптографических алгоритмов защиты; критерии оценки

Шифр компетенции	Индикаторы достижения компетенций	Шифр результата обучения	Результат обучения
	методов машинного обучения		качества построенных криптографических алгоритмов;
		У(ПК-4и-22Г)	Уметь: определять необходимые криптографические средства для защиты информации; использовать криптографические методы и способы защиты в локальных и глобальных вычислительных сетях, базах данных, интернет технологиях и системах искусственного интеллекта;
		В(ПК-4и-22Г)	Владеть: навыками анализа структуры и свойств алгоритмов шифрования; спецификой формирования требований по криптографической информации и выбору средств криптографической защиты информации; современными отечественными и зарубежными симметричные и асимметричными криптографическими шифрами;

3. Структура дисциплины

3.1. Виды учебной работы и трудоемкость (всего и по семестрам, в часах)

Форма обучения: очная

Вид учебной работы	Всего и по семестрам, часы	1	2	3	4	5	6	7	8	9	10	11	12
Контактная работа, всего в том числе:	**50**						50						

лекции (всего)	**16**						16						
-в т.ч. лекции on-line курс	**0**												
практические занятия (ПЗ)	**16**						16						
-в т.ч. практические занятия on-line курс	**0**												
лабораторные работы (ЛР)	**12**						12						
контролируемая самостоятельная работа (защита курсового проекта, курсовой работы и др. работ (при наличии))	**0**												
-в т.ч. лабораторные работы on-line курс	**0**												
иная контактная работа (сдача зачета, экзамена,консультации)	**6**						6						
проектная деятельность (ПД)	**0**												
Самостоятельная работа обучающихся (СРО), всего в том числе: (указать конкретный вид СРО)	**58**						58						
выполнение и подготовка к защите курсового проекта или курсовой работы	**0**												
выполнение и подготовка к защите РГР работы, реферата, патентных исследований, аналитических исследований и т.п	**0**												
изучение учебного материала, вынесенного на самостоятельную проработку	**21**						21						
подготовка к лабораторным и/или практическим занятиям	**14**						14						
подготовка к сдаче зачета, экзамена	**23**						23						
иные виды работ обучающегося (при наличии)	**0**												
освоение on-line курса	**0**												
самостоятельная проектная деятельность (СПД)	**0**												
ИТОГО ПО ДИСЦИПЛИНЕ	**108**						108						

4. Содержание дисциплины

4.1. Темы (разделы) дисциплины и виды занятий (в часах)

Форма обучения: очная

Номер темы (раздела)	Название темы (раздела)	Семестр	Трудоемкость, часы					Шифр результата обучения
			Л	ПЗ	ЛР	СРО	Всего	
1	Криптография и криптографические системы	6	4			14	**18**	З(ПК-4и-22Г) З(ПК-2и-22Г)
2	Симметричные криптосистемы	6	4	6	6	16	**32**	У(ПК-4и-22Г) У(ПК-2и-22Г) В(ПК-4и-22Г) В(ПК-2и-22Г)
3	Асимметричные криптосистемы	6	4	6	4	15	**29**	У(ПК-4и-22Г) У(ПК-2и-22Г) В(ПК-4и-22Г) В(ПК-2и-22Г)
4	Программно-аппаратные криптографические средства защиты	6	4	4	2	13	**23**	У(ПК-2и-22Г) В(ПК-2и-22Г)
	ИТОГО:		16	16	12	58	**102**	

4.2. Содержание лекционного курса

№ пп.	Номер раздела	Название темы	Трудоемкость, часы		
			очная	очно-заочная	заочная
1	1-Криптография и криптографические системы	**Основные понятия и определения криптографии** Принципы криптографии. Криптология и криптоанализ. Ключи шифрования. Криптологические системы.	2		
2	1-Криптография и криптографические системы	**Математические основы криптографии** Классы сложности алгоритмов. Делимость и алгоритм Евклида. Разложение числа на множители. Модулярная арифметика. Квадратичные вычеты. Закон взаимности и китайская теорема об остатках. Односторонние функции. Однонаправленные хэш-функции. Генераторы псевдослучайных чисел.	2		
3	2-Симметричные криптосистемы	**Методы симметричного шифрования** Простейшие методы шифрования с закрытым ключом. Общая схема симметричного шифрования. Методы замены. Пропорциональные шифры. Многоалфавитные подстановки. Методы гаммирования. Методы перестановки. Понятие композиционного шифра. Операции, используемые в блочных алгоритмах симметричного шифрования.	2		
4	2-Симметричные криптосистемы	**Современный отечественные и зарубежные симметричные шифры** Классическая сеть Фейстеля. Абсолютно надежный шифр. Основные свойства симметричных криптосистем. Алгоритм криптографического преобразования данных ГОСТ 28147-89. 3DES, AES, Blowfish, IDEA, Threefish.	2		
5	3-Асимметричные криптосистемы	**Основные свойства асимметричных криптосистем** Предпосылки создания методов шифрования с открытым ключом и основные определения. Требования к алгоритмам шифрования с открытым ключом. Использование асимметричных алгоритмов для шифрования. Цифровая подпись на основе алгоритмов с от-крытым ключом. Генерация и хранение ключей. Формирование секретных ключей с использованием асимметричных алгоритмов. Распределение ключей.	2		
6	3-Асимметричные криптосистемы	**Управление ключами в системах с открытым ключом** Алгоритм Диффи-Хелмана. Алгоритм RSA. Алгоритм Эль-Гамаля. Криптографические системы на эллиптических кривых. Возможные атаки при использовании алгоритмов асимметричного шифрования.	2		
7	4-Программно-аппаратные криптографические средства защиты	**Прикладные программные интерфейсы, реализующие средства защиты информации** Инфраструктура открытых ключей. Защищенные транспортные протоколы. Системы программной защиты.	2		
8	4-Программно-аппаратные криптографические средства защиты	**Программно-аппаратные средства защиты информации** Защищенный протокол HTTPS. Вопросы безопасности в Интернет протоколах. Системы аппаратной защиты.	2		
	-	**ИТОГО:**	16		

4.3. Перечень лабораторных работ

Номер раздела	№ ЛР	Название лабораторной работы	Трудоемкость, часы		
			очная	очно-заочная	заочная
2-Симметричные криптосистемы	1	**Шифры гаммирования и колонной замены** Сложение по модулю N. Сложение по модулю 2. Алгоритм Блюм-Блюм-Шуба. Шифровальные машины.	2		
2-Симметричные криптосистемы	2	**Шифр сложной замены, многоалфавитные замены** Шифр Гронсфельда, Бэкона, Книжный шифр, Вернама.	2		
2-Симметричные криптосистемы	3	**Алгоритм шифрования DES** Электронная кодовая книга ECB (Electronic Code Book); сцепление блоков шифра CBC (Cipher Block Chaining); обратная связь по шифртексту CFB (Cipher Feed Back); обратная связь по выходу OFB (Output Feed Back).	2		
3-Асимметричные криптосистемы	4	**Программная реализация MD5 и SHA-1** Основные этапы алгоритмов MD5, SHA-1 при сжатии исходного текста.	2		
3-Асимметричные криптосистемы	5	**Цифровая подпись** Изучение системы цифровой подписи Эль-Гамаля.	2		
4-Программно-аппаратные криптографические средства защиты	6	**Контроль целостности (биты четности, контрольные цифры, CRC и ECC)** Алгоритм Луна; Штрихкод по стандарту EAN-13; Заграничный паспорт гражданина РФ с биометрическими данными; индивидуальный номер налогоплательщика.	2		
-		**ИТОГО:**	12		

4.4. Перечень практических занятий

Номер раздела	№ ПЗ	Тема практического занятия	Трудоемкость, часы		
			очная	очно-заочная	заочная
2-Симметричные криптосистемы	1	**Традиционные симметричные криптосистемы** Шифр Цезаря, Магический квадрат, Вижинера, Трисемуса.	2		
2-Симметричные криптосистемы	2	**Современные отечественные симметричные алгоритмы** Сеть Фейстеля, отечественные блочные шифры, используемые в современных протоколах. ГОСТ 28147-89 и шифр "Магма", шифр «Кузнечик» (ГОСТ Р 34.12-2015). Режимы работы блочных шифров (ГОСТ Р 34.13-2015).	2		
2-Симметричные криптосистемы	3	**Современные зарубежные симметричные алгоритмы** Алгоритмы 3DES, AES, Blowfish, IDEA, Threefish.	2		
3-Асимметричные криптосистемы	4	**Шифр Шамира** Тайные многосторонние вычисления и разделение секрета по схеме Шамира.	2		
3-Асимметричные криптосистемы	5	**Асимметричный алгоритм Эль-Гамаля** Процедура создания ключей. Электронная цифровая подпись. Комбинированные криптосистемы.	2		
3-Асимметричные криптосистемы	6	**Асимметричный алгоритм RSA** Процедура создания ключей в RSA. Электронная цифровая	2		

		подпись.			
4-Программно-аппаратные криптографические средства защиты	7	**Применение СЗИ от НСД для организации защищенных компь-ютерных систем** Идентификация и аутентификация пользователей. Сетевые протоколы.	2		
4-Программно-аппаратные криптографические средства защиты	8	**Криптографические протоколы** Схема аутентификации Шнорра; протокол подбрасывания монеты; протоколы распределения ключей (ПРК): протоколы передачи сгенерированных ключей; протоколы совместной выработки общего ключа; протоколы предварительного распределения ключей.	2		
-		**ИТОГО:**	16		

4.5. Виды СРО

Номер раздела	Вид СРО	Трудоемкость, часы		
		очная	очно-заочная	заочная
1-Криптография и криптографические системы	подготовка к сдаче зачета, экзамена	8		
1-Криптография и криптографические системы	изучение учебного материала, вынесенного на самостоятельную проработку	6		
2-Симметричные криптосистемы	подготовка к сдаче зачета, экзамена	5		
2-Симметричные криптосистемы	подготовка к лабораторным и/или практическим занятиям	6		
2-Симметричные криптосистемы	изучение учебного материала, вынесенного на самостоятельную проработку	5		
3-Асимметричные криптосистемы	подготовка к сдаче зачета, экзамена	5		
3-Асимметричные криптосистемы	подготовка к лабораторным и/или практическим занятиям	5		
3-Асимметричные криптосистемы	изучение учебного материала, вынесенного на самостоятельную проработку	5		
4-Программно-аппаратные криптографические средства защиты	подготовка к сдаче зачета, экзамена	5		
4-Программно-аппаратные криптографические средства защиты	подготовка к лабораторным и/или практическим занятиям	3		
4-Программно-аппаратные криптографические средства защиты	изучение учебного материала, вынесенного на самостоятельную проработку	5		
-	ИТОГО:	58		

Темы для самостоятельной работы обучающихся

Раздел 1. Криптография и криптографические системы

Основные понятия термины и определения. Простейшие шифры. Шифры сдвига и замены.

Композиции шифров. Модели шифров. Блочные и поточные шифры. Понятие криптосистемы. Ключевая система шифра. Основные требования к шифрам.

Раздел 2. Симметричные криптосистемы

Классические криптосистемы. Шифры сложно замены, перестановки, шифры гаммирования. Композиционные шифры, сети Файстеля. Криптосистемы DES и отечественного ГОСТа. Стандарт криптографической защиты AES. Криптографическая стойкость шифров. Основные атаки на симметричные шифры. Совершенные шифры.

Раздел 3. Асимметричные криптосистемы

Ключевые системы. Схема открытого распределения ключей Диффи-Хеллмана. K5A. Криптосистема Рабина. Криптосистема Эль-Гамаля. Сравнение двух классов криптосистем, гибридные криптосистемы. Принципы криптоанализа, критерии распознавания открытого текста, универсальные методы криптоанализа. Алгоритм RSA. Криптографические хеш-функции. Электронная цифровая подпись.

Раздел 4. Программно-аппаратные криптографические средства защиты

Прикладные программные интерфейсы, реализующие средства защиты информации. Инфраструктура открытых ключей. Защищенные транспортные протоколы. Программно-аппаратные средства защиты информации.

5. Формы текущего контроля успеваемости и проведения промежуточной аттестации

Перечень оценочных средств текущего контроля и промежуточной аттестации по дисциплине приведен Фонде оценочных средств (приложение Б).

6. Учебно-методическое и информационное обеспечение дисциплины

6.1.Учебно-методическое обеспечение

Сведения об обеспеченности дисциплины основной, дополнительной и учебно-методической литературой приведены в формах № 1-УЛ и № 2-УЛ (приложение А).

6.2.Перечень современных профессиональных баз данных и информационных справочных систем, рекомендуемых для освоения дисциплины

Названия современных профессиональных баз данных и информационных справочных систем, рекомендуемых для освоения дисциплины	Ссылки на официальные сайты
https://standartgost.ru/	Открытая база ГОСТов
ЭБС Znanium.com	http://znanium.com/
ЭБС Лань	https://e.lanbook.com/
ЭБС «Университетская библиотека онлайн»	https://biblioclub.ru/
Электронная библиотека УГНТУ	http://www.bibl.rusoil.net

7. Материально-техническое обеспечение дисциплины

7.1. Перечень специальных аудиторий, кабинетов, лабораторий и пр., используемых при реализации дисциплины с перечнем основного оборудования

№ пп.	Номер помещения	Оснащенность помещения (перечень основного оборудования)	Наименование помещения

1	1-333	Компьютер тип К2 i3-3220/21,5" LG 22EA63T-P(8);Монитор 20" Acer(1);Системный блок UNIVERSAL D1(13);Доступ к электронной информационно-образовательной среде (Корпоративная информационная система УГНТУ); Доступ в интернет;	Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечено доступом в электронную информационно-образовательную среду организации.
2	1-333	Компьютер тип К2 i3-3220/21,5" LG 22EA63T-P(8);Монитор 20" Acer(1);Системный блок UNIVERSAL D1(13);Столы, стулья	Лаборатория – оснащенная лабораторным оборудованием, в зависимости от степени сложности.
3	1-420в	Компьютер Intel Core 2 Duo E8200(1);Компьютер WIN i3-550(2);Компьютер персональный i3-4170/21,5" PHILIPS 226V4LAB(2);Монитор 19" Acer(1);Монитор ASUS VA24DQ Black 23,8", шт(3);Принтер лазерный HP Laser Jet 3055 <Q6503A>(1);Сервисное устройство д\очистки Katun 3 м(1);Системный блок Intel Core i3-2100(1);Шкаф(ы) для хранения	Помещения для хранения и профилактического обслуживания учебного оборудования
4	1-435	Компьютер Pegatron Nettop MiniPC Wall-e L6(12);Компьютер тип К2 i3-3220/21,5" LG 22EA63T-P(1);Монитор Samsung S-LC24F390FHIXCI(9);Монитор Samsung S-LC24FG73FQIXCI(5);Проектор Optoma EH334(1);Системный блок UNIVERSAL D1(14);Столы, стулья	Учебная аудитория для проведения занятий семинарского типа – укомплектована специализированной (учебной) мебелью, техническими средствами обучения.
5	1-435	Компьютер Pegatron Nettop MiniPC Wall-e L6(12);Компьютер тип К2 i3-3220/21,5" LG 22EA63T-P(1);Монитор Samsung S-LC24F390FHIXCI(9);Монитор Samsung S-LC24FG73FQIXCI(5);Проектор Optoma EH334(1);Системный блок UNIVERSAL D1(14);Учебно-наглядные пособия по дисциплине,набор демонстрационного оборудования; Столы, стулья;	Учебная аудитория для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).
6	1-435	Компьютер Pegatron Nettop MiniPC Wall-e L6(12);Компьютер тип К2 i3-3220/21,5" LG 22EA63T-P(1);Монитор Samsung S-LC24F390FHIXCI(9);Монитор Samsung S-LC24FG73FQIXCI(5);Проектор Optoma EH334(1);Системный блок UNIVERSAL D1(14);Столы, стулья	Учебная аудитория для текущего контроля и промежуточной аттестации – укомплектована специализированной (учебной) мебелью, техническими средствами обучения.
7	1-435	Компьютер Pegatron Nettop MiniPC Wall-e L6(12);Компьютер тип К2 i3-3220/21,5" LG 22EA63T-P(1);Монитор Samsung S-LC24F390FHIXCI(9);Монитор Samsung S-LC24FG73FQIXCI(5);Проектор Optoma EH334(1);Системный блок UNIVERSAL D1(14);Столы, стулья	Учебная аудитория для проведения групповых и индивидуальных консультаций
8	1-435	Компьютер Pegatron Nettop MiniPC Wall-e L6(12);Компьютер тип К2 i3-3220/21,5" LG 22EA63T-P(1);Монитор Samsung S-LC24F390FHIXCI(9);Монитор Samsung S-LC24FG73FQIXCI(5);Проектор Optoma EH334(1);Системный блок UNIVERSAL D1(14);Столы, стулья	Лаборатория – оснащенная лабораторным оборудованием, в зависимости от степени сложности.

9	1-444	Компьютер Nettop Pegatron Walle L6 PV D-SUB(1);Настенный экран Master Picture 244x244 MW(1);Проектор Acer ProjectorP1203(1);мультимедиапроектор;Учебно-наглядные пособия по дисциплине,набор демонстрационного оборудования; Столы, стулья;	Учебная аудитория для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).
10	3-201	Защитная RFID Система LSG405HF(1);Компьютер i3-2120(1);Компьютер i3-3220 K1 BenQ 21,5"(4);Компьютер i3-3240 21.5" Acer(2);Компьютер ПК НИКС\i3-4170\21.5"(1);Компьютер персональный-нettоп Celeron J1900/4Gb(1);Контрольно-кассовая машина Пионер 114Ф с ФН(1);МФУ hp Laser Jet Pro M1132<CE847A>A4(1);МФУ hp LaserJet Pro M1132<CE847A>(A4 принтер+сканер+копир)(1);Монитор Beng(1);Принтер Laser Jet 1020(1);Сканер Plustek Optic Book 4800(1);Универсальная RFID станция книговыдачи/программирования меток(3);Чековый принтер АТОЛ RP-326-USE черный Rev.6(3);Ящик каталожный 40 ячеек(5);Доступ к электронной информационно-образовательной среде (Корпоративная информационная система УГНТУ); Доступ в интернет;	Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечено доступом в электронную информационно-образовательную среду организации.

7.2. Перечень лицензионного и свободно распространяемого программного обеспечения, используемых в учебном процессе при освоении дисциплины

№ пп.	Наименование ПО	Лицензионная чистота (реквизиты лицензии,свидетельства о гос. регистрации и т.п., срок действия)
1	Microsoft Office Professional Plus	Дата выдачи лицензии 23.11.2020, Поставщик: ООО «Компарекс»
2	Microsoft WinPro 10, WINHOME 10	Дата выдачи лицензии 23.11.2020, Поставщик: ООО «Компарекс»
3	Антивирус Kaspersky	Дата выдачи лицензии 27.10.2010

8. Организация обучения лиц с ограниченными возможностями здоровья

Для лиц с ограниченными возможностями здоровья, обучающихся по данной образовательной программе, разрабатывается индивидуальная программа освоения дисциплины с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья.

Приложение А

Форма № УЛ-1

СВЕДЕНИЯ
об обеспеченности дисциплины основной и дополнительной учебной литературой

Наименование дисциплины: (48547)Криптографические алгоритмы

Направление подготовки (специальность): 09.03.01 Информатика и вычислительная техника

Направленность: профиль«Технологии искусственного интеллекта в нефтегазовой отрасли»

Форма обучения: очная;

Кафедра, обеспечивающая преподавание дисциплины: Вычислительная техника и инженерная кибернетика (ВТИК);

Тип	Назначение учебных изданий	Семестр			Библиографическое описание	Кол-во экз.	Адрес нахождения электронного учебного издания	Коэффициент обеспеченности
		очная	очно-заочная	заочная				
1	2	3	4	5	6	7	8	9
Основная литература	Для выполнения СРО;Для изучения теории;	6			Игнатьев, Е. Б. Основы криптографии : учебное пособие / Е. Б. Игнатьев. — Иваново : ИГЭУ, 2020. — 88 с. — Текст : электронный. — URL: https://e.lanbook.com/book/154559 (дата обращения: 06.10.2022).	1	http://www.e.lanbook.com	1.00
Дополнительная литература	Для изучения теории;	6			Романьков, В. А. Введение в криптографию : курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 240 с. — Текст : электронный. - URL: https://znanium.com/catalog/product/1514566 (дата обращения: 06.10.2022).	1	http://www.znanium.com	1.00
Дополнительная литература	Для выполнения СРО;Для выполнения практических занятий;Для изучения теории;	6			Пономарчук, Ю. В. Основы анализа шифров классической криптографии : учебное пособие / Ю. В. Пономарчук. — Хабаровск : ДВГУПС, 2019. — 113 с. — Текст : электронный. — URL: https://e.lanbook.com/book/179357 (дата обращения: 06.10.2022).	1	http://www.e.lanbook.com	1.00
Примечание – Графы 1-5,8 заполняются кафедрой, графы 7 и 9 - библиотекой								

Составил: доцент, канд. физ.-мат. наук Хизбуллина С.Ф.
Год приема 2023 г.

Форма № УЛ-2

СВЕДЕНИЯ
об обеспеченности дисциплины учебно-методическими изданиями

Наименование дисциплины: (48547)Криптографические алгоритмы

Направление подготовки (специальность): 09.03.01 Информатика и вычислительная техника

Направленность профиль«Технологии искусственного интеллекта в нефтегазовой отрасли»

Форма обучения очная;

Кафедра, обеспечивающая преподавание дисциплины: Вычислительная техника и инженерная кибернетика (ВТИК);

Назначение учебных изданий	Семестр			Библиографическое описание	Кол-во экз.		Адрес нахождения электронного учебного издания	Коэффициент обеспеченности
	очная	очно-заочная	заочная		Всего	в том числе на кафедре		
1	2	3	4	5	6	7	8	9
Для выполнения лабораторных работ;	6			Криптографические методы защиты компьютерной информации : учебно-методическое пособие к выполнению лабораторных работ по методам и средствам защиты компьютерной информации / УГНТУ, каф. ВТИК ; сост.: Т. Х. Агишев, В. Н. Филиппов. - Уфа : Изд-во УГНТУ, 2012. - 494 Кб. - URL: http://bibl.rusoil.net/base_docs/UGNTU/VTIK/Agishev1.pdf. - Текст : электронный.	1	0	http://bibl.rusoil.net	1.00
Для выполнения СРО;Для выполнения практических занятий;	6			Стеганографические методы встраивания скрытой служебной информации : учебно-методическое пособие по выполнению практических работ по методам и средствам защиты компьютерной информации / УГНТУ, каф. ВТИК ; сост.: Т. Х. Агишев, В. Н. Филиппов. - Уфа : Изд-во УГНТУ, 2012. - 748 Кб. - URL: http://bibl.rusoil.net/base_docs/UGNTU/VTIK/Agishev2.pdf. - Текст : электронный.	1	0	http://bibl.rusoil.net	1.00
Примечание – Графы 1-5,8 заполняются кафедрой, графы 6,7 и 9 - библиотекой								

Составил:
доцент, канд. физ.-мат. наук Хизбуллина С.Ф.

Год приема 2023 г.

Приложение Б

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уфимский государственный нефтяной технический университет»

Фонд оценочных средств по текущей успеваемости и промежуточной аттестации по дисциплине

Криптографические алгоритмы

Направление подготовки (специальность): 09.03.01 Информатика и вычислительная техника

Направленность: профиль «Технологии искусственного интеллекта в нефтегазовой отрасли»

Уровень высшего образования: бакалавриат

Форма обучения: очная;

Кафедра, обеспечивающая преподавание дисциплины: Вычислительная техника и инженерная кибернетика (ВТИК);

Трудоемкость дисциплины: 3 з.е. (108час)

Уфа

ФОС по текущей успеваемости и промежуточной аттестации по дисциплине разработал (и):

доцент, канд. физ.-мат. наук Хизбуллина С.Ф.

Рецензент
доцент, канд. физ.-мат. наук Зарипов Д.М.

ФОС по текущей успеваемости и промежуточной аттестации по дисциплине рассмотрен и одобрен на заседании кафедры Вычислительная техника и инженерная кибернетика (ВТИК), обеспечивающей преподавание дисциплины 31.08.2022, протокол №1.

И.о. Заведующий кафедрой
Вычислительная техника и инженерная кибернетика (ВТИК) Д.М. Зарипов

СОГЛАСОВАНО

И.о. Заведующий кафедрой ВТИК Д.М. Зарипов

Год приема 2023 г.

ФОС по текущей успеваемости и промежуточной аттестации по дисциплине
зарегистрирован 19.09.2022 № 1 в отделе УРО и внесен в электронную базу данных

1. Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Шифр результата обучения	Результат обучения	Индикатор достижения компетенций	Показатели достижения результатов освоения компетенций	Вид оценочного средства
1	Криптография и криптографические системы	З(ПК-2и-22Г)	основные криптографические стандарты; принципы построения криптографических алгоритмов и использования в информационных системах и системах искусственного интеллекта;	ПК-2.1. Настраивает программное обеспечение и участвует в разработке программных компонентов систем искусственного интеллекта	перечисляет принципы построения криптографических алгоритмов и использования в информационных системах и системах искусственного интеллекта	Письменный и устный опрос Тестирование
		З(ПК-4и-22Г)	требования к криптографическим системам защиты информации; понятие и виды криптографических атак; виды криптографических алгоритмов защиты; критерии оценки качества построенных криптографических алгоритмов;	ПК-4.1. Проводит анализ требований и определяет необходимые классы задач машинного обучения	перечисляет основные требования к системам криптографической защиты;	Письменный и устный опрос Тестирование
				ПК-4.2. Определяет метрики оценки результатов моделирования и критерии качества построенных моделей	перечисляет основные алгоритмы криптографической защиты;	Письменный и устный опрос Тестирование
				ПК-4.3. Принимает участие в оценке, выборе и при необходимости	называет критерии оценки при выборе криптографических	Письменный и устный

				разработке методов машинного обучения	алгоритмов, в том числе и для методов машинного обучения;	опрос Тестирование
2	Симметричные криптосистемы	В(ПК-2и-22Г)	основные криптографические стандарты; принципы построения криптографических алгоритмов и использования в информационных системах и системах искусственного интеллекта;	ПК-2.1. Настраивает программное обеспечение и участвует в разработке программных компонентов систем искусственного интеллекта	разрабатывает и настраивает программное обеспечение с использованием методов шифрования и криптоанализа при построении современных симметричных криптосистем	Лабораторная работа Письменный и устный опрос Тестирование
		В(ПК-4и-22Г)	требования к криптографическим системам защиты информации; понятие и виды криптографических атак; виды криптографических алгоритмов защиты; критерии оценки качества построенных криптографических алгоритмов;	ПК-4.1. Проводит анализ требований и определяет необходимые классы задач машинного обучения	применяет методы обеспечения помехоустойчивости и имитозащиты в сетях засекреченной сявзи	Лабораторная работа Письменный и устный опрос Тестирование
				ПК-4.2. Определяет метрики оценки результатов моделирования и критерии качества построенных моделей	разрабатывает программные компоненты криптографических систем и оценивает их эффективность	Лабораторная работа Письменный и устный опрос Тестирование

				ПК-4.3. Принимает участие в оценке, выборе и при необходимости разработке методов машинного обучения	демонстрирует навыки программной реализации алгоритмов симетричного шифрования	Лабораторная работа Письменный и устный опрос Тестирование
		У(ПК-2и-22Г)	основные криптографические стандарты; принципы построения криптографических алгоритмов и использования в информационных системах и системах искусственного интеллекта;	ПК-2.1. Настраивает программное обеспечение и участвует в разработке программных компонентов систем искусственного интеллекта	выбирает оптимальный режим работы алгоритма симметричного шифрования;	Лабораторная работа Письменный и устный опрос Тестирование
		У(ПК-4и-22Г)	требования к криптографическим системам защиты информации; понятие и виды криптографических атак; виды криптографических алгоритмов защиты; критерии оценки качества построенных криптографических алгоритмов;	ПК-4.1. Проводит анализ требований и определяет необходимые классы задач машинного обучения	анализирует и интерпретирует структуры и основные характеристики современных симметричных шифров	Лабораторная работа Письменный и устный опрос Тестирование
				ПК-4.2. Определяет метрики оценки результатов моделирования и	выбирает необходимые режимы работы симметричных алгоритмов для	Лабораторная работа Письменн

				критерии качества построенных моделей	решения практических задач	ый и устный опрос Тестирование
				ПК-4.3. Принимает участие в оценке, выборе и при необходимости разработке методов машинного обучения	оценивает криптостойкость симметричных алгоритмов	Лабораторная работа Письменный и устный опрос Тестирование
3	Асимметричные криптосистемы	В(ПК-2и-22Г)	основные криптографические стандарты; принципы построения криптографических алгоритмов и использования в информационных системах и системах искусственного интеллекта;	ПК-2.1. Настраивает программное обеспечение и участвует в разработке программных компонентов систем искусственного интеллекта	разрабатывает и настраивает программное обеспечение с использованием методов шифрования и криптоанализа при построении современных ассимметричных криптосистем	Лабораторная работа Письменный и устный опрос Тестирование
		В(ПК-4и-22Г)	требования к криптографическим системам защиты информации; понятие и виды криптографических атак; виды криптографических алгоритмов защиты;	ПК-4.1. Проводит анализ требований и определяет необходимые классы задач машинного обучения	применяет методы создания скрытого канала передачи данных средствами криптографии с открытым ключом	Лабораторная работа Письменный и устный опрос Тестиров

			критерии оценки качества построенных криптографических алгоритмов;			ание
				ПК-4.2. Определяет метрики оценки результатов моделирования и критерии качества построенных моделей	применяет программные компоненты криптографических систем для оценки их эффективности	Лабораторная работа Письменный и устный опрос Тестирование
				ПК-4.3. Принимает участие в оценке, выборе и при необходимости разработке методов машинного обучения	демонстрирует навыки программной реализации алгоритмов ассиметричного шифрования	Лабораторная работа Письменный и устный опрос Тестирование
		У(ПК-2и-22Г)	основные криптографические стандарты; принципы построения криптографических алгоритмов и использования в информационных системах и системах искусственного интеллекта;	ПК-2.1. Настраивает программное обеспечение и участвует в разработке программных компонентов систем искусственного интеллекта	выбирает оптимальный режим работы алгоритма ассимметричного шифрования;	Лабораторная работа Письменный и устный опрос Тестирование
		У(ПК-4и-22Г)	требования к криптографическим	ПК-4.1. Проводит анализ требований и	анализирует и интерпретирует	Лабораторная

			системам защиты информации; понятие и виды криптографических атак; виды криптографических алгоритмов защиты; критерии оценки качества построенных криптографических алгоритмов;	определяет необходимые классы задач машинного обучения	структуры и основные характеристики современных ассимметричных шифров	работа Письменный и устный опрос Тестирование
				ПК-4.2. Определяет метрики оценки результатов моделирования и критерии качества построенных моделей	выбирает необходимые режимы работы ассимметричных алгоритмов для решения практических задач	Лабораторная работа Письменный и устный опрос Тестирование
				ПК-4.3. Принимает участие в оценке, выборе и при необходимости разработке методов машинного обучения	оценивает криптостойкость ассимметричных алгоритмов	Лабораторная работа Письменный и устный опрос Тестирование
4	Программно-аппаратные криптографические средства защиты	В(ПК-2и-22Г)	основные криптографические стандарты; принципы построения криптографических алгоритмов и использования в	ПК-2.1. Настраивает программное обеспечение и участвует в разработке программных компонентов систем искусственного	демонстрирует навыки работы в программном обеспечении КриптоАРМ и КриптоПро; устанавливает программные	Лабораторная работа Письменный и устный опрос

			информационных системах и системах искусственного интеллекта;	интеллекта	криптографические средства защиты информации	Тестирование
		У(ПК-2и-22Г)		ПК-2.1. Настраивает программное обеспечение и участвует в разработке программных компонентов систем искусственного интеллекта	классифицирует основные принципы и механизмы криптозащиты	Лабораторная работа Письменный и устный опрос Тестирование

2. Перечень оценочных средств для текущего контроля и промежуточной аттестации по дисциплине

п/п	Вид оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде	Шкала оценки
1	2	3	4	5
1	Лабораторная работа	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по лабораторным исследованиям	Темы, задания для выполнения ла-бораторных работ; вопросы и тре-бования к их защите	оценка «*отлично*» выставляется обучающемуся, если задание по работе выполнено в полном объеме; точно отвечает на контрольные вопросы; отчет выполнен аккуратно и в соответствии с предъявляемыми требованиями; при выполнении работы обучающийся продемонстрировал отличный уровень владения умениями и навыками при решении профессиональных задач в рамках усвоенного учебного материала; оценка «*хорошо*» выставляется обучающемуся, если задание по работе выполнено в полном объеме; отвечает на дополнительные теоретические вопросы, испытывая небольшие затруднения; качество оформления отчета к работе не полностью соответствует требованиям; при выполнении работы обучающийся продемонстрировал хороший уровень владения умениями и навыками при решении профессиональных задач в рамках усвоенного учебного материала; оценка «*удовлетворительно*» выставляется

				обучающемуся, если задание по работе выполнено в неполном объеме; работа выполнена с небольшими неточностями; при защите на дополнительные вопросы было допущено несколько неправильных ответов; не может полностью объяснить полученные результаты; при выполнении работы обучающийся продемонстрировал удовлетворительный уровень владения умениями и навыками при решении профессиональных задач в рамках усвоенного учебного материала; оценка «*неудовлетворительно*» выставляется обучающемуся, если задание по работе выполнено в неполном объеме; при выполнении работы обучающийся продемонстрировал недостаточный уровень владения умениями и навыками при решении профессиональных задач в рамках усвоенного учебного материала; при защите на дополнительные вопросы были даны неправильные ответы, а ряд вопросов остался без ответов;
2	Письменный и устный опрос	Оценочное средство для текущего контроля успеваемости и промежуточной аттестации. Позволяет выявить и восполнить пробелы в знаниях; повторить, закрепить, систематизировать материал; оценить знания, умения, теоретические и практические навыки; определить уровень сформированных у студентов компетенций по дисциплине (модулю)	Совокупность вопросов, заданий, упражнений, тестов для выполнения контрольных работ, домашних заданий, РГР и иных учебных работ. Комплект билетов для текущей и промежуточной аттестации	оценка «*отлично*» выставляется обучающемуся, если обучающийся правильно ответил на теоретические вопросы; показал отличные знания в рамках усвоенного учебного материала; ответил на все дополнительные вопросы; оценка «*хорошо*» выставляется обучающемуся, если обучающийся ответил на теоретические вопросы с небольшими неточностями; показал хорошие знания в рамках усвоенного учебного материала; ответил на большинство дополнительных вопросов; оценка «*удовлетворительно*» выставляется обучающемуся, если обучающийся ответил на теоретические вопросы с существенными неточностями; показал удовлетворительные знания в рамках усвоенного учебного материала; при ответах на дополнительные вопросы было допущено несколько неправильных ответов; оценка «*неудовлетворительно*» выставляется обучающемуся, если при ответе на теоретические вопросы обучающийся продемонстрировал недостаточный уровень знаний; на дополнительные вопросы отвечает неправильно;
3	Тестирование	Система стандартизированных простых и комплексных заданий, позволяющая автоматизировать процедуру измерения уровня знаний, умений и владений	Фонд тестовых заданий.	оценка «*отлично*» выставляется обучающемуся, если обучающийся дал правильные ответы на 80…100 % вопросов; оценка «*хорошо*» выставляется обучающемуся, если обучающийся дал правильные ответы на 60…79 % вопросов;

		обучающегося.		оценка «*удовлетворительно*» выставляется обучающемуся, если обучающийся дал правильные ответы на 40…59 % вопросов; оценка «*неудовлетворительно*» выставляется обучающемуся, если обучающийся дал правильные ответы менее 40 %;

Приложение В

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уфимский государственный нефтяной технический университет»

Письменный и устный опрос.

Перечень вопросов (задач, заданий, тем, комплекта тестовых заданий):

Краткие вопросы:
1. Продолжите фразу: «Криптографическое преобразование информации – это взаимно-однозначное математическое преобразование, зависящее от …»
Ответ: ключа.
2. Продолжите фразу: «Процесс извлечения открытого текста из криптограммы при условии значения ключа называется …»
Ответ: расшифрованием.
3. Продолжите фразу: «Шифры, осуществляющие преобразование информации порциями фиксированной длины, составленными из подряд идущих символов сообщения, называются …»
Ответ: блочными.
4. Заполните пропуски: «Все криптографические преобразования могут быть сведены к операциям двух базовых типов: … и …»
Ответ: замены, перестановки.
5. Продолжите фразу: «Блочными являются классические шифры: …»
Ответ: перестановки.
6. Продолжите фразу: «В шифре гаммирования гаммой называется …»
Ответ: ключ.
7. Заполните пропуски: «Электромеханические шифровальные машины на подобие «Энигма» основаны на использовании шифра … замены»
Ответ: колонной.
8. Продолжите фразу: «Шифра сложной замены являются …»
Ответ: многоалфавитными.
9. Заполните пропуски: «Криптосистема Энигма является шифром … замены»
Ответ: сложной.
10. Заполните пропуски: «Симметричные шифры являются … криптосистемами»
Ответ: одноключевыми
11. Заполните пропуски: «Увеличение количества раундов алгоритма шифрования обычно приводит к … его эффективности»
Ответ: снижению.
12. Заполните пропуски: «Увеличение количества раундов обычно приводит к … стойкости алгоритма шифрования»
Ответ: повышению.
13. Заполните пропуски: «Алгоритм … имеет структуру «квадрат»»
Ответ: ГОСТ 28147-89.
14. Заполните пропуски: «Алгоритм шифрования … не имеет слабых ключей»
Ответ: AES.
15. Заполните пропуски: «Алгоритм AES в процессе шифрования оперирует с …»
Ответ: байтами.
16. Заполните пропуски: «Длина ключа современного симметричного шифра должна составлять не менее … бит для обеспечения практической стойкости»
Ответ: 128.
17. Найти значение функции Эйлера ?(26) = …?
Ответ: 12
18. Найти значение функции Эйлера ?(39) = …?

Ответ: 24
19. Найти значение функции Эйлера ?(35) = …?
Ответ: 24
20. Найти значение функции Эйлера ?(34) = …?
Ответ: 16
21. Найти значение функции Эйлера ?(77) = …?
Ответ: 60
22. Заполните пропуски: «Значение функции Эйлера от N определяется как … натуральных чисел в ряду от 1 до N-1, взаимно простых с N»
Ответ: количество.
23. Продолжите фразу: «Наиболее распространенной на практике системой шифрования с открытым ключом является шифр …»
Ответ: RSA
24. Заполните пропуски: «Для обеспечения практической стойкости длина ключа криптосистемы RSA должна быть не менее …бит»
Ответ: 1024
25. Заполните пропуски: «Для обеспечения эквивалентной стойкости ключ ассиметричной криптосистемы должен быть … ключа симметричного шифра»
Ответ: длиннее

Перечень вопросов к экзамену:
1. Шифры одноалфавитной замены. Шифр Цезаря, квадрат «Полибия».
2. Асимметричная криптография и электронная цифровая подпись.
3. Аппаратное шифрование DES: структура, перестановки, сеть Фейстеля, расширение ключа.
4. Шифры перестановки. Квадрат «Кардана».
5. Шифры многоалфавитной замены. Табло Виженера.
6. IDEA: структура, алгоритм, расширение ключа.
7. Шифровальный аппарат Вернама. Шифр Вернама (XOR).
8. Структура ГОСТ 28147-89: образующая функция, расширение ключа.
9. Шифр Плейфейера.
10. Классификация шифров по ключевой информации.
11. Алгоритм шифрования AES.
12. Шифр Хилла.
13. Типы криптоанализа шифрованных сообщений. Понятие защищенности шифрованных сообщений.
14. Основные принципы асимметричной криптографии.
15. Нелинейные поточные шифры. Фильтрующие шифры. Линейный регистр сдвига.
16. Комбинирующие поточные шифры. Корреляционно-стойкий комбинирующий шифр.
17. Динамический поточный шифр.
18. Определение блочного шифрования. Блок информации. Ключ алгоритма. Абсолютно симметричный блочный шифр.
19. Аутентификация пользователя. Типы систем аутентификации (на симметричных и асимметричных криптосистемах, на сертификатах).
20. Kerberos. Протокол распределения ключей.
21. Распространение ключей. Протоколы, основанные на использовании симметричной криптосистемы и случайных параметров.
22. Распространение ключей. 3-х этапный протокол Шамира (Shamir).
23. Классическая структура сети Фейстеля. Ветви сети, материал ключа, раунд сети, образующая функция.
24. Распространение ключей. Протоколы на основе асимметричных криптосистем.
25. Алгоритм RSA (асимметричная криптография).
26. Алгоритм открытого распределения ключей Диффи-Хелмана.
27. Аутентификация пользователей как основной компонент межсетевых экранов.

28. Программные методы защиты сетевых технологий в Internet структурах.
29. Защита данных в электронных платежных системах.
30. Принципы функционирования электронных платежных систем.
31. Персональный идентификационный номер (PIN). Обеспечение безопасности электронно-платежной системы POS (Point-of-Sale), схема функционирования POS.
32. Обеспечение безопасности электронных платежей через сеть Internet.
33. Авторизация и шифрование финансовой информации в сети Internet.
34. Протоколы шифрования SSL (Secure Socket Layer) и SET (Secure Electronic Transactions), использование сертификатов.
35. Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.
36. Криптографические протоколы.
37. Классификация криптографических протоколов.
38. Основные элементы криптографических протоколов.
39. Протоколы обмена ключами.
40. Защищенные транспортные протоколы.
41. Защищенный протокол HTTPS.

Приведенные выше вопросы, формируют комплект билетов для проведения промежуточной аттестации (экзамена), например:

Экзаменационный билет №00
по дисциплине "Криптографические алгоритмы"
Направление подготовки: 09.03.01 "Информатика и вычислительная техника"
Профиль: «Технологии искусственного интеллекта в нефтегазовой отрасли»

1. Аппаратное шифрование DES: структура, перестановки, сеть Фейстеля, расширение ключа.
2. Классификация криптографических протоколов.

Лабораторная работа.

Перечень вопросов (задач, заданий, тем, комплекта тестовых заданий):

Лабораторная работа №1. Шифры гаммирования и колонной замены
Задача: разработка программного кода для алгоритма сложение по модулю N; сложение по модулю 2; алгоритм Блюм-Блюм-Шуба.

Лабораторная работа №2. Шифр сложной замены, многоалфавитные замены
Задача: разработка программного кода, реализующего шифры: Гронсфельда, Бэкона, Книжный шифр, Вернама.

Лабораторная работа №3. Алгоритм шифрования DES.
Задача: программная реализация режимов: электронная кодовая книга ECB (Electronic Code Book); сцепление блоков шифра CBC (Cipher Block Chaining); обратная связь по шифртексту CFB (Cipher Feed Back); обратная связь по выходу OFB (Output Feed Back).

Лабораторная работа №4 Программная реализация MD5 и SHA-1
Задача: программная реализация алгоритмов MD5, SHA-1 при сжатии исходного текста.

Лабораторная работа №5. Цифровая подпись
Задача: Изучение системы цифровой подписи Эль-Гамаля.

Лабораторная работа №6. Контроль целостности (биты четности, контрольные цифры, CRC и ECC)
Задача: реализация алгоритма Луна; штрихкод по стандарту EAN-13; заграничный паспорт

гражданина РФ с биометрическими данными; индивидуальный номер налогоплательщика.

Методика выполнения лабораторных работ приведены в учебно-методических пособиях:
URL: http://bibl.rusoil.net/base_docs/UGNTU/VTIK/Agishev1.pdf;
http://bibl.rusoil.net/base_docs/UGNTU/VTIK/Agishev2.pdf

Тестирование.

Перечень вопросов (задач, заданий, тем, комплекта тестовых заданий):

1. Криптография - это наука о методах:
а) кодирования информации
б) и алгоритмах шифрования
в) вскрытия шифров
2. Предметом криптоанализа являются методы:
а) имитозащиты сообщений
б) шифрования данных
в) вскрытия шифров
3. Криптограммой называется:
а) результат шифрования
б) шифрующая система
в) секретный параметр шифра
4. Стеганография – это наука о методах:
а) шифрования при условии секретности алгоритма шифра
б) скрытия факта передачи секретного сообщения
в) дешифрования сообщения без знания ключа
5. Имитозащита – это защита системы секретной связи от:
а) вскрытия шифра
б) перехвата сообщений
в) навязывания ложных сообщений
6. шифром замены является:
а) «Скитала»
б) «Квадрат Полибия»
в) «Решетка Кардано»
7. Перестановочным шифром является:
а) шифр Цезаря
б) шифр Вижинера
в) Решетка Кардано
8. Шифром сложной замены является:
а) шифр Цезаря
б) шифр Вижинера
в) омофонический шифр
9. Шифром простой замены является:
а) омофонический шифр
б) шифр гаммирования
в) шифр колонной замены
10. Шифр гаммирования заключается:
а) в маршрутной перестановке символов
б) в замене символов по таблице
в) в сложении по модулю с символами случайной последовательности
11. В абсолютно стойком шифре Виженера ключ должен быть:
а) абсолютно случайным

б) многоразовым
в) циклическим
12. Стойкость современных симметричных композиционных шифров, таких как DES, базируется:
а) на реализации принципов рассеивания и перемешивания
б) на секретности алгоритма шифрования
в) на бесконечности ключевой последовательности
13. S-блоком симметричного блочного алгоритма шифрования называется:
а) циклический сдвиг блока битов
б) таблица перестановки битов в блоке
в) таблица замены группы битов
14. Алгоритм DES использует операцию:
а) сложения по модулю 2^16
б) циклического сдвига
в) подстановки с помощью S-блоков
15. Алгоритмы DES и ГОСТ 28147-89 имеют структуру:
а) «квадрат»
б) подстановочно-перестановочная сеть
в) сеть Фейстеля
16. Число раундов алгоритма AES определяется:
а) размером входного блока
б) длиной ключа
в) содержимым входного блока
17. Отечественный шифр «Кузнечик», определенный в ГОСТ Р 34.12-2012, имеет структуру:
а) «квадрат»
б) сеть Фейстеля
в) SP-сеть
18. Режим работы шифров … производит шифрование и расшифрование блоков текста независимо друг от друга
а) электронная кодовая книга ECB
б) сцепление блоков шифротекста CBC
в) обратная связь по шифротексту CFB
19. Ключи, которые являются разными, но приводят к одному и тому же результату шифрования, называются:
а) слабыми
б) комплементарными
в) эквивалентными
20. Ключи, при использовании которых стойкость алгоритма шифрования существенно снижается, называются:
а) слабыми
б) комплементарными
в) скомпрометированными
21. Асимметричные криптосистемы являются:
а) бесключевыми
б) одноключевыми
в) двухключевыми
22. В случае применения ассиметричной криптосистемы отправитель сообщения использует для шифрования:
а) свой открытый ключ
б) свой личный ключ
в) открытый ключ получателя
г) личный ключ получателя
23. Криптосистема Диффи-Хеллмана является протоколом:
а) шифрования

б) распределения ключей
в) электронной подписи
г) взаимной аутентификации
24. Технология цифровой подписи использует хэш-значение, вычисленное:
а) для открытого сообщения
б) для открытого ключа
в) для личного ключа
25. Российским стандартом функции хэширования является:
а) ГОСТ 34.10-2012
б) ГОСТ 28147-89
в) ГОСТ Р 34.11-2012
26. К многоключевым криптосистемам относят системы:
а) разделения секрета
б) доказательства с нулевым разглашением
в) хэшиирования
27. Алгоритм RSA генерирует … в качестве цифровой подписи сообщения:
а) пару чисел
б) новое сообщение двойной длины
в) одно число
28. Цифровая подпись по алгоритму … является детерминированной:
а) DSA
б) RSA
в) Эль-Гамаля
29. Расширенный алгоритм Евклида используется в ассиметричных криптосистемах для решения задач:
а) факторизации числа
б) нахождения числа, обратного заданному по модулю
в) быстрого возведения в степень по модулю
30. Основной проблемой практического использования ассиметричных криптосистем является:
а) проблема распределения ключей
б) невозможность аутентификации отправителя
в) низкая производительность

Аннотация к рабочей программе дисциплины

Криптографические алгоритмы

Направление подготовки (специальность): 09.03.01 Информатика и вычислительная техника

Направленность: профиль«Технологии искусственного интеллекта в нефтегазовой отрасли»

Уровень высшего образования: бакалавриат

Форма обучения: очная;

Кафедра, обеспечивающая преподавание дисциплины: Вычислительная техника и инженерная кибернетика (ВТИК);

Компетенции, формируемые в результате освоения дисциплины

ПК-2и-22Г Способен разрабатывать и тестировать программные компоненты решения задач в системах искусственного интеллекта:

-ПК-2.1. Настраивает программное обеспечение и участвует в разработке программных компонентов систем искусственного интеллекта

ПК-4и-22Г Способен разрабатывать и применять методы машинного обучения для решения задач:

-ПК-4.1. Проводит анализ требований и определяет необходимые классы задач машинного обучения

-ПК-4.2. Определяет метрики оценки результатов моделирования и критерии качества построенных моделей

-ПК-4.3. Принимает участие в оценке, выборе и при необходимости разработке методов машинного обучения

Результат обучения

Знать:

ПК-2и-22Г-2 основные криптографические стандарты; принципы построения криптографических алгоритмов и использования в информационных системах и системах искусственного интеллекта;

ПК-4и-22Г-2 требования к криптографическим системам защиты информации; понятие и виды криптографических атак; виды криптографических алгоритмов защиты; критерии оценки качества построенных криптографических алгоритмов;

Уметь:

ПК-2и-22Г-2 решать задачи, связанные с кодированием и защитой информации, настраивать и запускать основные виды криптографического программного обеспечения, направленных на защиту безопасности компьютерной информации;

ПК-4и-22Г-2 определять необходимые криптографические средства для защиты информации; использовать криптографические методы и способы защиты в локальных и глобальных вычислительных сетях, базах данных, интернет технологиях и системах искусственного интеллекта;

Владеть:

ПК-2и-22Г-2 криптографическими методами обеспечения секретности, генерации и

распределения ключевой информации, обеспечения целостности и аутентификации; правилами криптографического преобразования для хранения информации в вычислительных системах; вопросами безопасности в Интернет протоколах, системами аппаратной защиты;
ПК-4и-22Г-2 навыками анализа структуры и свойств алгоритмов шифрования; спецификой формирования требований по криптографической информации и выбору средств криптографической защиты информации;
современными отечественными и зарубежными симметричные и асимметричными криптографическими шифрами;

Краткая характеристикадисциплины

Криптография и криптографические системы; Симметричные криптосистемы; Асимметричные криптосистемы; Программно-аппаратные криптографические средства защиты;

Трудоёмкость (з.е. / часы)

3 з.е. (108час)

Вид промежуточной аттестации

экзамен;

Разработчик(и):

доцент, канд. физ.-мат. наук Хизбуллина С.Ф.

СОГЛАСОВАНО
И.о. Заведующий кафедрой ВТИК Д.М. Зарипов