

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины
Криптографические методы защиты информации

Направление подготовки (специальности)
10.03.01 Информационная безопасность

Направленность (профиль)
«Безопасность компьютерных систем»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 18 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

1. Цели освоения дисциплины

Целью изучения дисциплины является овладение базовыми понятиями и методами в области криптографической защиты информации, овладение современным математическим аппаратом, используемым в криптографии для дальнейшего использования в приложениях.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Криптографические методы защиты информации» относится к обязательной части образовательной программы.

Дисциплина играет важную роль для профессиональной подготовки специалиста. При ее изучении используются знания, полученные при изучении математических дисциплин «Алгебра», "Теория чисел", "Дискретная математика", "Информатика" и "Математическая логика и теория алгоритмов". Знания, умения и навыки, полученные при изучении дисциплины "Криптографические методы защиты информации", используются обучаемыми при изучении профессиональных и специальных дисциплин.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Общепрофессиональные компетенции		
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИД-ОПК-9_1 Понимает корректность криптографических алгоритмов в современных программных комплексах ИД-ОПК-9_2 Способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям	Знать: - основные задачи, решаемые криптографическими методами; - математические модели шифров, подходы к оценке их стойкости; - основные типы криптопротоколов и принципов их построения с использованием шифрсистем; - основные протоколы идентификации и аутентификации абонентов сети; - защитные механизмы и средства обеспечения сетевой безопасности. Уметь: - корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; - применять математические методы при исследовании криптографических алгоритмов. Владеть: - навыками использования типовых криптографических алгоритмов; - подходами к разработке и анализу безопасности криптографических протоколов.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 акад. часа.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам) Формы ЭО и ДОТ (при наличии)
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Введение	7	2	4				4	Задания для самостоятельной работы
2	Элементы шифрования	7	2	4				4	Задания для самостоятельной работы
3	Элементы криптоанализа	7	1	4		1		2	Задания для самостоятельной работы
4	Модели систем шифрования	7	1					2	Задания для самостоятельной работы
5	Простейшие шифры	7	1	6		1		4	Задания для самостоятельной работы Контрольная работа №1
6	Дискретный логарифм	7	1	6		1		4	Задания для самостоятельной работы
7	Шифрование с открытым ключом	7	2	6		1		4	Задания для самостоятельной работы
8	Генерация псевдослучайных последовательностей	7	1	4				2	Задания для самостоятельной работы
9	Поточные криптосистемы	7	1	2		1		2	Задания для самостоятельной работы
10	Идентификация и аутентификация	7	1	4		1		4	Задания для самостоятельной работы Контрольная работа №2
11	Электронная подпись	7	1	4		1		2	Задания для самостоятельной работы

12	Электронные платежи	7	1	2		1		2	Задания для самостоятельной работы
13	Управление ключами	7	1	2					
						2	0,5	33,5	Экзамен
	ИТОГО		16	48		10	0,5	69,5	
	<i>в том числе с ЭО и ДОТ</i>								

Содержание разделов дисциплины:

1. Введение

Основные задачи в области обеспечения информационной безопасности, решаемые криптографическими методами. Краткий исторический обзор криптографических методов защиты информации. Исторические примеры шифров: шифр Цезаря, квадрат Полибия, шифр Плейфейра, решетка Кардано, книжный шифр.

2. Элементы шифрования

Алфавит. Оцифровка. Платформы шифрования. Хэш-функции. Функция шифрования. Шифр замены. Блочный шифр. Шифр перестановки. Функция XOR. Шифр Вернама. Гаммирование. Режимы использования блочных шифров. Стандарты блочного шифрования DES и AES.

3. Элементы криптоанализа

Понятие криптоанализа. Атаки, типы атак. Полный перебор. Частотный анализ.

4. Модели систем шифрования

Вероятностная модель К.Шеннона. Совершенная секретность. Мера теоретической секретности.

5. Простейшие шифры

Аффинный шифр. Шифр Хилла. Шифр Виженера. Их криптостойкость. Тест Казисского определения длины ключа в шифре Виженера.

6. Дискретный логарифм

Проблема дискретного логарифма. Протоколы, основанные на трудности нахождения дискретного логарифма: протоколы Диффи - Хеллмана, Масси – Омуры, Эль Гамала. Атаки на дискретный логарифм.

7. Шифрование с открытым ключом

Понятие шифрования с открытым ключом. Криптосистема RSA. Сложные задачи, обеспечивающие криптостойкость RSA. Правильный выбор параметров. Битовая стойкость RSA. Потребность в простых числах. Проверка на простоту, тест Миллера – Рабина. Построение больших простых чисел. Разложимость целых чисел на множители. Метод фактор-баз Ферма.

8. Генерация псевдослучайных последовательностей

Равномерно распределенная случайная последовательность. Понятие псевдослучайной последовательности. Генерация псевдослучайных последовательностей. Линейный и мультипликативный конгруэнтный генераторы. Генератор псевдослучайных последовательностей, основанный на системе RSA. Генератор псевдослучайных

последовательностей Микали – Шнорра. Генератор BBS псевдослучайных последовательностей.

9. Поточные криптосистемы

Синхронные и самосинхронизирующиеся поточные криптосистемы. Линейный регистр сдвига с обратной связью. Периодичность его выпускных последовательностей.

10. Идентификация и аутентификация

Понятия идентификации и аутентификации. Доказательство с нулевым разглашением. Протокол Фиата – Шамира.

11. Электронная подпись

Основные требования к электронной подписи. Подпись на базе RSA. Электронная подпись Эль Гамала. Слабости алгоритмов. Стандарты электронной подписи.

12. Электронные платежи

Требования к электронным деньгам. Технология электронного платежа. Исторически первый пример данной технологии – Master Card.

13. Управление ключами

Симметричные и асимметричные системы шифрования. Задачи управления ключами. Распределение ключей. Протокол Цербер.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

В процессе обучения используются следующие технологии электронного обучения и дистанционные образовательные технологии:

Электронный учебный курс «КМЗИ» в LMS Электронный университет Moodle ЯрГУ, в котором:

- представлены задания для самостоятельной работы обучающихся по темам дисциплины;
- осуществляется проведение отдельных мероприятий текущего контроля успеваемости студентов;
- представлены тексты лекций по отдельным темам дисциплины;
- представлены правила прохождения промежуточной аттестации по дисциплине;
- представлен список учебной литературы, рекомендуемой для освоения дисциплины;
- представлена информация о форме и времени проведения консультаций по дисциплине в режиме онлайн;
- посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:
для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTeX;
- Adobe Acrobat Reader.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используется Автоматизированная библиотечно-информационная система «БУКИ-NEXT»
http://www.lib.uniyl.ac.ru/opac/bk_cat_find.php

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2022. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/489242> (дата обращения: 22.01.2022).
2. Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург : Лань, 2021. — 400 с. — ISBN 978-5-8114-1116-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/167921> (дата обращения: 22.01.2022). — Режим доступа: для авториз. пользователей.

б) дополнительная литература

1. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/489487> (дата обращения: 22.01.2022).
2. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие / М. А. Иванов, И. В. Чугунков. — Москва : НИЯУ МИФИ, 2012. — 400 с. — ISBN 978-5-7262-1676-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/75810> (дата обращения: 22.01.2022). — Режим доступа: для авториз. пользователей.
3. Романьков, В. А. Введение в криптографию: курс лекций. / В. А. Романьков - М.: ФОРУМ, 2012. - 239 с.
3. Гашков, С. Б. Криптографические методы защиты информации: учеб. пособие для вузов. / С. Б. Гашков, Э. А. Применко, М. А. Черепнев; УМО по классическому университет. образованию - М.: Академия, 2010. - 298 с.

в) ресурсы сети «Интернет»

1. Электронные каталоги НБ ЯрГУ http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php
2. Электронная библиотека учебных материалов ЯрГУ
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

Доцент кафедры алгебры
и математической логики, к. ф.-м. н. М.Е. Сорокина

Приложение № 1 к рабочей программе дисциплины «Криптографические методы защиты информации»

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Задания для самостоятельной работы

(данные задания выполняются студентом самостоятельно
и преподавателем в обязательном порядке не проверяются)

Задания по теме № 1 «Введение»:

Зашифровать (расшифровать) сообщения шифром Цезаря, шифром квадрат Полибия, шифром Плейфейра, с помощью решетки Кардано.

Задания по теме № 2 «Элементы шифрования»:

- 1) Алфавит русский. Текст разбит на блоки длины $n=10$. Буквы внутри каждого блока переставляются перестановкой $s=(1\ 5\ 10)(2\ 8\ 3\ 7\ 6)(4\ 9)$. Зашифровать текст, расшифровать текст.
- 2) Представить текст в виде бинарной последовательности и зашифровать его с помощью шифра Вернама, придумав свой ключ.
- 3) Расшифровать данный текст, зашифрованный шифром Вернама, зная ключ шифрования.
- 4) Зашифровать (расшифровать) текст с помощью гаммирования, алфавит русский (английский), оцифровка стандартная.
- 5) Самостоятельно разобрать в представленной литературе стандарты шифрования DES и AES.

Задания по теме № 3 «Элементы криптоанализа»:

- 1) Расшифровать текст, зашифрованный простой заменой (алфавит русский – 33 буквы).
- 2) Расшифровать текст, зашифрованный простой заменой (алфавит русский – 32 буквы).
- 3) Расшифровать текст, зашифрованный простой заменой (алфавит английский).

Задания по теме № 4 «Модели систем шифрования»:

Разобрать материал по данному разделу в

Задания по теме № 5 «Простейшие шифры»:

- 1) Выбрать язык (алфавит) и матрицу шифрования шифром Хилла порядка 3 и зашифровать фразу «Моя фамилия. . .».
- 2) Расшифровать следующий текст, зашифрованный шифром Хилла (алфавит русский – 33 буквы). Известны матрица шифрования порядка 3

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 4 \\ 1 & 2 & 2 \end{pmatrix}$$

и нулевой вектор, используемые для шифрования. Зашифрованный текст:

Г Н Г Н Ъ Д Л Н В П Ъ М Е Щ Ъ

- 3) Пусть E_1 - шифрование шифром Виженера с длиной ключа 12 и E_2 – шифрование шифром Виженера с длиной ключа 22. Что можно сказать о двукратном шифровании E_1E_2 ?
- 4) Построить шифр Виженера с длиной ключа не менее 5, выбрать фразу длины не менее 50 знаков, оцифровать ее и зашифровать, используя построенный шифр. Привести вычисления длины ключа, использующие тест Казисского, вычислить значения функции Казисского для прореженных текстов. Соответствуют ли вычисления теории?
- 5) Известно, что шифрограмма получена шифром Виженера. Найти длину ключа. Найти ключ. Расшифровать сообщение.

Задания по теме № 6 «Дискретный логарифм»:

- 1) Вычислить методом Сильвера - Полига - Хеллмана дискретный логарифм элемента 25 в поле F_{41} относительно порождающего элемента $g = 7$.
- 2) Построить поле F_{7^3} . Найти порождающий элемент g его мультипликативной группы. Вычислить дискретный логарифм $\log_g f$ по основанию g элемента $f=5x^2+2x+6$ методом Сильвера - Полига – Хеллмана.
- 3) Построить конкретный протокол Диффи - Хеллмана с платформой F_{27} .

Задания по теме № 7 «Шифрование с открытым ключом»:

- 1) Пусть дана система RSA с модулем $n = 77$. Сколько всего имеется ключей шифрования e ? Сколько из них совпадает со своими ключами дешифрования d ?
- 2) Пусть дана система RSA с модулем $n = 18857$ и ключом шифрования $e = 18421$. Алфавит английский (26 букв) в стандартной нумерации. Единицы исходного текста – 3-графы. Шифрованный текст: 1975, 2416, 5531, 9161, 17705, 280, 10645, 11810, 17908, 15682, 12955, 1775. Найти ключ дешифрования d . Расшифровать.
- 3) Проверить, будет ли простым число 8563496351.
- 4) Разложить на множители число 384628056762.

Задания по теме № 8 «Генерация псевдослучайных последовательностей»:

- 1) Вывести формулу для общего члена последовательности, порождаемой ЛКГ $x_{t+1}=ax_t+b \pmod n$.
- 2) Выяснить, когда ЛКГ из предыдущей задачи порождает последовательность максимального периода.
- 3) Проиллюстрировать работу генератора псевдослучайных последовательностей, основанного на системе RSA, для модуля $n=51$ и ключа шифрования $e=4$.
- 4) Проиллюстрировать работу генератора BBS псевдослучайных последовательностей для модуля $n=243$.

Задания по теме № 9 «Поточные криптосистемы»:

- 1) Показать, что многочлен $f(x)=x^4+x^3+1 \in \mathbb{Z}_2[x]$ неприводим. Будет ли он примитивным? Чему равен период выпускной последовательности LFSR с таким связующим многочленом?
- 2) Проверить, что неприводимый многочлен $f(x)=x^5+x^2+1 \in \mathbb{Z}_2[x]$ является примитивным. Убедиться, что в качестве связующего многочлена он дает выпускную последовательность максимального периода 31, выбрав вектором начальных содержаний $[1, 1, 1, 1, 1]$.
- 3) Построить LFSR максимального периода с длиной регистра 6.

Задания по теме № 10 «Идентификация и аутентификация»:

Продemonстрировать работу протокола Фиата – Шамира на примере $p=5$, $q=11$.

Задания по теме № 11 «Электронная подпись»:

- 1) Продemonстрировать выполнение алгоритма электронной подписи на базе RSA. В качестве M , M_s и S взять Z_n , функция R – сдвиг на одну позицию, $p_A=61$, $q_A=17$, $e_A=101$ – ключ шифрования, документ $m=247$.
- 2) Продemonстрировать выполнение алгоритма электронной подписи Эль Гамала для $p=17$, $a=9$ – долгосрочный ключ. Документ $m=10110$.

Задания по теме № 12 «Электронные платежи»:

Продemonстрировать технологию электронного платежа на примере Master Card для $p=7$, $q=11$, $e=19$ – открытый ключ шифрования, клиент А выбирает $x=10$.

Контрольная работа № 1

(проверка сформированности ОПК-9, индикаторы ИД-ОПК_9_1 и ИД-ОПК-9_2)

Примеры заданий:

1. Найти $37^{-1} \pmod{91}$.
2. Найти все образующие мультипликативной группы конечного поля F_8 .
3. Известны исходный текст и текст, полученный из него шифром Хилла. Алфавит английский – 26 букв, занумерованных от 0 до 25. Известно, что матрица шифрования имеет порядок 2. Вектор, используемый при шифровании, неизвестен. Восстановить ключ шифрования.

cryptography \leftrightarrow 2, 17, 24, 15, 19, 14, 6, 17, 0, 15, 7, 24.

Контрольная работа № 2

(проверка сформированности ОПК-9, индикаторы ИД-ОПК_9_1 и ИД-ОПК-9_2)

Примеры заданий:

1. Пусть $F_{16} = Z_2[x]/(x^4+x+1)$. Найти в F_{16} обратный элемент к a^3+a^2+1 , где a – образ x при гомоморфизме $Z_2[x] \rightarrow Z_2[x]/(x^4+x+1)$.
2. Найти все образующие мультипликативной группы конечного поля F_{11} .
3. Продemonстрировать работу протокола Фиата – Шамира на примере $p=11$, $q=13$.

Правила выставления оценки по результатам контрольной работы

Оценка по результатам контрольной работы считается в баллах по каждому заданию по следующему принципу:

- правильно выполненное задание – 1 балл;
- при выполнении задания правильно применены теоретические факты, понятия и алгоритмы дисциплины, но имеются ошибки в численных расчетах – 0,8 балла;

- при выполнении задания правильно применены теоретические факты, понятия и алгоритмы дисциплины, указан план дальнейшего решения, но задание выполнено не до конца – 0,6 балла;

- при выполнении задания студент обнаруживает ошибки в знании теоретических фактов или понятий дисциплины, применяет неправильный алгоритм действий – 0 баллов.

Набранное количество баллов 3 соответствует оценке «отлично», 2,4 – 2,8 баллов – оценке «хорошо», 1,8 - 2,2 балла – оценке «удовлетворительно», менее 1,8 баллов – оценке «неудовлетворительно» (умения и навыки на данном этапе освоения дисциплины не сформированы).

2. Список вопросов и заданий для проведения промежуточной аттестации

Список вопросов к экзамену

1. Исторические примеры шифров: шифр Цезаря, квадрат Полибия, решетка Кардано, книжный шифр.
2. Платформа шифрования. Алфавит. Оцифровка. Хэш-функция.
3. Шифр замены. Шифр перестановки.
4. Шифр Вернама. Гаммирование.
5. Режимы использования блочных шифров.
6. Криптоанализ. Полный перебор. Частотный анализ.
7. Теоретическая стойкость шифров по К. Шеннону.
8. Аффинный шифр, шифр Хилла.
9. Шифр Виженера. Тест Казисского и определение с его помощью длины ключа в шифре Виженера. Роторные машины.
10. Дискретный логарифм. Протокол Диффи - Хеллмана.
11. Протокол Масси – Омуры. Протокол Эль Гамала.
12. Атаки на дискретный логарифм. Алгоритм Сильвера – Полига – Хеллмана.
13. Криптосистема RSA.
14. Сложные задачи, обеспечивающие криптостойкость RSA.
15. Проверка натуральных чисел на простоту. Тест Миллера – Рабина.
16. Построение больших простых чисел.
17. Разложимость целых чисел на множители. Метод фактор-баз Ферма.
18. Генерация псевдослучайных последовательностей. Линейные и мультипликативные конгруэнтные генераторы.
19. Генератор псевдослучайных последовательностей, основанный на системе RSA.
20. Генератор псевдослучайных последовательностей Микали – Шнорра, генератор BBS.
21. Поточные криптосистемы: синхронные, самосинхронизирующиеся.
22. Линейный регистр сдвига с обратной связью (LFSR). Периодичность и статистика выпускных последовательностей LFSR.
23. Идентификация и аутентификация. Пароль, пин, одноразовые пароли, многократная идентификация.
24. Доказательства с нулевым разглашением. Протокол Фиата – Шамира.
25. Электронная подпись. Подпись на базе RSA.
26. Электронная подпись Эль Гамала.
27. Стандарт DSS электронной подписи.
28. Стандарт ГОСТ Р 34.10-94 электронной подписи.
29. Электронные платежи. Master Card.
30. Управление ключами. Протокол Цербер.

31. Стандарт шифрования DES.

32. Стандарт шифрования AES.

Список задач к экзамену

1. Нахождение НОД двух целых чисел с помощью алгоритма Евклида.
2. Нахождение линейного выражения НОД двух целых чисел с помощью обобщенного алгоритма Евклида.
3. Решение систем сравнений при помощи Китайской теоремы об остатках.
4. Действия с вычетами в кольце Z_n (возведение в степень, нахождение обратного).
5. Построение конечного поля и выполнение алгебраических операций в нем.
6. Нахождение образующих элементов мультипликативной группы конечного поля.
7. Нахождение порядка элемента или всех элементов данного порядка мультипликативной группы конечного поля (или мультипликативной группы кольца вычетов по модулю n).

Правила выставления оценки на экзамене

В экзаменационный билет включается два теоретических вопроса и задача. На подготовку к ответу дается не менее 1 часа.

По итогам экзамена выставляется одна из оценок: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Оценка «Отлично» выставляется студенту, который демонстрирует глубокое и полное владение содержанием материала и понятийным аппаратом дисциплины, умеет связывать теорию с практикой. Студент дает развернутые, полные и четкие ответы на вопросы экзаменационного билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала, грамотно использует терминологию.

Оценка «Хорошо» выставляется студенту, ответ которого на экзамене в целом соответствуют указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора.

Оценка «Удовлетворительно» выставляется студенту, который дает недостаточно полные и последовательные ответы на вопросы экзаменационного билета и дополнительные вопросы, но при этом демонстрирует умение выделить существенные и несущественные признаки и установить причинно-следственные связи. Ответы излагаются в терминах дисциплины, но при этом допускаются ошибки в определении и раскрытии некоторых основных понятий, формулировке положений, которые студент затрудняется исправить самостоятельно. При аргументации ответа студент не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется студенту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой, допускает грубые ошибки при определении сущности раскрываемых понятий, явлений, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется также студенту, который взял экзаменационный билет, но отвечать отказался.

Приложение № 2 к рабочей программе дисциплины «Криптографические методы защиты информации»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Криптографические методы защиты информации» являются лекции; по всем темам предусмотрены практические занятия, на которых происходит закрепление лекционного материала путем применения его к конкретным задачам и отработка навыков работы с математическим аппаратом.

Для успешного освоения дисциплины очень важно решение достаточно большого количества задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия и основные методы дисциплины.

Задания для самостоятельного решения формулируются на лекциях и практических занятиях. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач. Полный список заданий для самостоятельной работы по темам (разделам) дисциплины приведен в ЭУК в LMS Moodle «КМЗИ». Вопросы, возникающие в процессе или по итогам решения этих задач, можно задать на консультациях и практических занятиях или в форуме (чате) в ЭУК в LMS Moodle.

Для самостоятельной работы, в том числе и повтора разобранного на лекциях и практических занятиях материала, рекомендуется использовать материалы, выложенные в ЭУК в LMS Moodle «КМЗИ».

В конце изучения дисциплины студенты сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса и задачу. На самостоятельную подготовку к экзамену выделяется 3 дня, в это время предусмотрена и групповая консультация.