

Время выполнения задания - 240 мин.

Задание 1. Дайте развернутые ответы на вопросы 1-5.

Вопрос 1.

Ваня и Петя используют следующую систему шифрования. Исходный текст, записанный без пробелов, разбивается последовательно на части по 10 букв. В каждой части буквы нумеруются слева направо от 1 до 10 и затем переставляются по правилу, которое задается в табл.2.

Таблица 2

1	2	3	4	5	6	7	8	9	10
7	9	8	1	3	2	4	10	6	5

То есть, первая буква каждой части ставится на 7 место, вторая – на 9 место и т.д. Однажды Ваня собрался отправить сообщение Пете. Он его зашифровал, а потом, для пущей надежности, зашифровал полученный текст еще раз. Подумал, и зашифровал его еще 333 раза. В результате Петя получил вот такое сообщение:

«СЪТУЕМНСЕЯИКЛЕОНКАСО».

Помогите Пете его прочитать.

Вопрос 2.

Опасно ли использовать мобильный банк? Что нужно сделать, чтобы снизить возникающие риски?

Вопрос 3.

Охарактеризуйте мошенничество в сфере компьютерной информации как категорию противоправного деяния.

Вопрос 4.

Что такое Agile и как его реализуют сейчас?

Вопрос 5

Сколько в среднем бит передаваемой информации оказывается искаженной в эфирной части передаваемой сотовой телефонной связи от телефона до радиовышки во время типичного грозового разряда, если скорость передачи $V=13$ Кбит/с?

Задание 2. Решите задачи

Задача 1.

81 раз бросается монета, при этом 60 раз выпал орел. Можно ли сказать, что монета правильная т.е. вероятность выпадения орла или решки одинакова и равна $\frac{1}{2}$?

Задача 2.

Расшифруйте текст, зашифрованный шифром перестановки, имея ключ

Текст: «ПОРИКТФЧРАГИА СКЕЯИААЦЗТ»

Ключ:

1	2	3	4	5	6
5	3	4	1	6	2

Задача 3.

Найдите все натуральные числа, оканчивающиеся на 2006, которые после зачеркивания последних четырех цифр уменьшаются в целое число раз.

Задача 4

Сколько в среднем бит передаваемой информации может быть искажено в эфирном тракте Wi-Fi при типичном грозовом разряде, если скорость V передачи данных составляет $V = 1 \text{ Mbit/s}$?

Задача 5

В пин-коде платежной карточки 4 цифры, каждая из которых выбирается случайно из множества $0,1, \dots, 9$ и независима друг от друга. Сколько в среднем будет одинаковых цифр в пин-коде?

Задание 3. Выберите один или несколько правильных ответов среди предложенных и заштрихуйте соответствующий овал в бланке ответов на пересечении номера вопроса и номера ответа. Дополнительно можете привести обоснование ответа..

Вопрос 1.

Как принято оформлять политику безопасности в организации:

- 1) в виде приказа о назначении ответственных лиц;
- 2) в виде отчетов обо всех действиях пользователей в АИС;
- 3) как документ, включающий описание проблемы, область применения, позиции руководства организации, санкции за не выполнение и пр.;
- 4) в виде инструкции о действиях в критических ситуациях.

Вопрос 2

В технологии электронной подписи используется пара ключей – открытый и закрытый. Каким ключом делается подпись:

- 1) открытым ключом отправителя;
- 2) открытым ключом получателя;
- 3) закрытым ключом отправителя;
- 4) закрытым ключом получателя.

Вопрос 3

Перехват сетевых пакетов, передаваемых по линиям передачи данных в сети это:

- 1) Dos-атака;
- 2) Спуфинг;
- 3) «Man-in-the-middle»;
- 4) Сниффинг.

Вопрос 4

Какая модель управления доступом является групповой:

- 1) на основе идентификации;
- 2) мандатная;
- 3) ролевая;
- 4) дискреционная.

Вопрос 5

Основой построения большинства поточных шифров являются:

- 1) генераторы псевдослучайных чисел, в частности, различные комбинации регистров сдвига;
- 2) схемы суммирования по mod 16;
- 3) таблицы подстановок.

Задание 4. Прочитайте раздел *Federal Information Security Management Act of 2002*, сделайте критический анализ на русском языке, определите соотношение указанных положений с правовыми нормами Российской Федерации.

SEC. 203. Compatibility of executive agency methods for use and acceptance of electronic signatures.

PURPOSE.—The purpose of this section is to achieve interoperable implementation of electronic signatures for appropriately secure electronic transactions with Government.

(b) ELECTRONIC SIGNATURES.—In order to fulfill the objectives of the Government Paperwork Elimination Act (Public Law 105-277;

112 Stat. 2681-749 through 2681-751), each Executive agency (as defined under section 105 of title 5, United States Code) shall ensure that its methods for use and acceptance of electronic signatures are compatible with the relevant policies and procedures issued by the Director.

(c) AUTHORITY FOR ELECTRONIC SIGNATURES.—The Administrator of General Services shall support the Director by establishing a framework to allow efficient interoperability among Executive agencies when using electronic signatures, including processing of digital signatures.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the General Services Administration, to ensure the development and operation of a Federated bridge certification authority for digital signature compatibility, and for other activities consistent with this section, \$8,000,000 or such sums as are necessary in fiscal year 2003, and such sums as are necessary for each fiscal year thereafter.

Задание 5. Выберите одну из предложенных тем и напишите эссе по этой теме:

1. Угрозы и риски в системе обеспечения информационной безопасности.
2. Флаги идентификаторов сессий (cookies) httponly и secure.
3. Какие на ваш взгляд должны быть основные принципы безопасной работы в интернете?