

**Спецификация конкурсных материалов для проведения практического этапа
Московского конкурса межпредметных навыков и знаний
«Интеллектуальный мегаполис. Потенциал» в номинации «ИТ-класс»
по направлению «Информационная безопасность»**

1. Назначение конкурсных материалов

Материалы практического этапа Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» (далее – Конкурс) предназначены для оценки уровня практической подготовки участников Конкурса.

2. Условия проведения практического этапа

Практический этап Конкурса проводится в форме компьютерного тестирования дистанционно. Во время выполнения работы не допускается использование вспомогательных материалов. Задачи при необходимости сопровождаются справочными комментариями. Разрешается использовать непрограммируемый калькулятор, а также среды разработки.

При выполнении работы обеспечивается строгое соблюдение порядка организации и проведения Конкурса.

3. Продолжительность выполнения работы

На выполнение заданий практического этапа Конкурса отводится **90 минут**. В процессе выполнения заданий предусмотрены **две** автоматические паузы продолжительностью по **5 минут** в соответствии с санитарно-эпидемиологическими требованиями к условиям и организации обучения в общеобразовательных организациях.

4. Содержание и структура работы

Задания практического этапа Конкурса разработаны преподавателями образовательных организаций высшего образования, участвующих в проекте «ИТ-класс в московской школе».

Индивидуальный вариант участника формируется автоматически во время проведения практического этапа Конкурса предпрофессиональных умений из базы конкурсных заданий.

Индивидуальный вариант участника включает 15 заданий, базирующихся на содержании элективного курса «Информационная безопасность».

5. Система оценивания отдельных заданий и работы в целом

Задание считается выполненным, если ответ участника совпал с эталоном. В работе используются задания двух типов: с выбором ответа и с кратким ответом. Максимальный балл за каждое задание выставляется в зависимости от указанного типа следующим образом:

- обычного уровня сложности с выбором одного ответа из нескольких предложенных – 3 балла;
- повышенного уровня сложности с кратким ответом – 6 баллов.

Максимальный балл за выполнение всех заданий – 60 баллов. Для получения максимального балла за практический этап Конкурса необходимо дать верные ответы на все задания.

6. Приложения

Приложение 1. Обобщённый план конкурсных материалов для проведения практического этапа Конкурса.

Приложение 2. Демонстрационный вариант конкурсных заданий практического этапа Конкурса.

**Обобщённый план конкурсных материалов
для проведения практического этапа Конкурса**

№ задания	Уровень сложности	Проверяемые темы	Контролируемые требования к проверяемым умениям	Балл
1	Базовый	Системы счисления	Умение выполнять переводы чисел в различные системы счисления	3
2	Базовый	Алгебра логики	Умение преобразовывать логические выражения, сопоставлять логические выражения на основе таблиц истинности	3
3	Базовый	Комбинаторика	Умение решать задачи с применением комбинаторных формул	3
4	Базовый	Основы теории информации	Умение рассчитывать количество информации, прибегая к вероятностному подходу	3
5	Базовый	Основы криптографии	Умение выполнять криптографические преобразования	3
6	Базовый	Основы криптоанализа	Умение восстанавливать неизвестные параметры криптографических преобразований	3
7	Базовый	Алгебра в кольцах вычетов	Умение вычислять выражения в кольцах вычетов	3
8	Базовый	Диофантовы уравнения	Умение решать диофантовы уравнения	3
9	Базовый	Китайская теорема об остатках	Умение решать системы линейных сравнений в кольцах вычетов	3
10	Базовый	Квадратичные сравнения в кольцах вычетов	Умение решать квадратичные сравнения в кольцах вычетов	3
11	Повышенный	Основы теории информации	Умение рассчитывать количество информации, прибегая к вероятностному подходу	6
12	Повышенный	Основы криптографии	Умение выполнять криптографические преобразования	6
13	Повышенный	Основы криптоанализа	Умение восстанавливать неизвестные параметры криптографических преобразований	6
14	Повышенный	Понятие делимости, простых чисел, НОД, НОК	Умение определять простые числа, вычислять НОД и НОК	6
15	Повышенный	IP-адресация	Знание и понимание принципов IP-адресации в сети	6

Сумма баллов: 60

**Демонстрационный вариант конкурсных заданий
практического этапа Московского конкурса межпредметных навыков и знаний
«Интеллектуальный мегаполис. Потенциал» в номинации «ИТ-класс» по
направлению «Информационная безопасность»**

Задача 1. Сколько существует натуральных значений $x \geq 2$, при которых справедливо тождество:

$$101_x = A25_{x-1} ?$$

Здесь нижний индекс указывает на основание системы счисления. А – цифра системы счисления.

- A. одно
- B. два
- C. ни одного

Ответ: C

Задача 2. Какая функция из предложенных вариантов тождественна выражению: $(a \vee \neg b) \rightarrow c$?

- A. $(a \vee b \vee c) (\neg a \vee b \vee c) (\neg a \vee \neg b \vee c)$
- B. $(a \vee b \vee c) (\neg a \vee b \vee c) (a \vee \neg b \vee \neg c)$
- C. $(a \vee b \vee c) (a \vee \neg b \vee c) (\neg a \vee b \vee \neg c)$

Ответ: A

Задача 3. Известно, что в качестве пароля используется трёхзначная троичная комбинация $x_1x_2x_3$, которая обладает следующим свойством: $x_1 = (x_2 + x_3) \bmod 3$. Сколько паролей в худшем случае придётся перебрать для определения правильного?

Операция $T \bmod P$ возвращает неотрицательный остаток от деления T на P .

- A. 8
- B. 12
- C. 27

Ответ: A

Задача 4. Дано сообщение: «Одновременно подкинули два одинаковых игральных кубика. На втором выпала грань с чётным значением». Используя формулу Шеннона, определите, сколько бит информации оно несёт?

- A. 0
- B. 1
- C. 2

Ответ: B

Задача 5. Какой шифртекст получится в результате применения перестановки 3-4-1-5-2 к слову ШИФРОВАНИЕ?

- A. ОВАНШИИЕФР
- B. ФРШОИНИВЕА
- C. ФРШОИВАННИЕ

Ответ: В

Задача 6. Известно, что для шифрования слова на русском языке был выбран такой шифр (ключ k неизвестен):

- буквы слова заменены на их порядковые номера в алфавите по схеме:

Буква	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Замена	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

- затем каждый такой номер n подвергли преобразованию до числа $m = 1 + (n - 1 + k) \bmod 33$;

- каждое полученное на предыдущем этапе число m вновь заменили по схеме из первого этапа.

В результате получилось следующее: ЫМШФТЁДСМИ. В ответе укажите применённый ключ k .

Операция $T \bmod P$ возвращает неотрицательный остаток от деления T на P .

- А. 13
- В. 7
- С. 4

Ответ: С

Задача 7. Чему равно значение следующего выражения в кольце вычетов \mathbb{Z}_{23} : $(10 + 7 \cdot 22) / 6$?

- А. 7
- В. 12
- С. 19

Ответ: В

Задача 8. Сколько существует целочисленных решений уравнения $13x - 18y = 2$ вида (x, y) , у которых x – положительное двузначное число?

- А. 5
- В. 7
- С. 8

Ответ: А

Задача 9. Решите систему сравнений и найдите наименьшие положительные x и y . В ответе укажите их сумму.

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{7} \\ y \equiv 4 \pmod{7} \\ y \equiv 0 \pmod{5} \end{cases}$$

Операция $T \bmod P$ возвращает неотрицательный остаток от деления T на P .

- А. 37
- В. 42
- С. 51

Ответ: В

Задача 10. Сколько решений есть у квадратичного сравнения: $5x^2 \equiv 3 \pmod{14}$?

Операция $T \bmod P$ возвращает неотрицательный остаток от деления T на P .

- A. 1
- B. 2
- C. 4

Ответ: B

Задача 11. Дано сообщение: «Подкинули три игральных кубика. На одном выпала грань с чётным значением, на двух других выпали грани одинаковой чётности». Используя формулу Шеннона, определите, сколько бит информации оно несёт? В ответе укажите целое число бит.

Ответ: 1

Задача 12. Зашифруйте число 131, проведя следующие манипуляции:

- перевод в троичную систему счисления;
- перестановка: 2-5-4-1-3.

Ответ: 12112

Задача 13. Известно, что используется криптосистема RSA, однако секреты были выбраны слабые. В результате опубликован открытый ключ $e = 17$ и модуль $m = 77$. В ответе укажите значение закрытого ключа системы d .

Ответ: 53

Задача 14. В ответе укажите наибольший общий делитель чисел 1890 и 5712.

Ответ: 42

Задача 15. В ответе укажите количество хостов, на которые рассчитана подсеть с маской 255.255.248.0.

Ответ: 2046