Пермский край

2024-2025 учебный год

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ПО ТРУДУ (ТЕХНОЛОГИИ)
МУНИЦИПАЛЬНЫЙ ЭТАП
10-11 КЛАСС

ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ТЕОРЕТИЧЕСКИЙ ТУР

Уважаемый участник олимпиады!

Вам предстоит выполнить теоретические задания. Время выполнения заданий теоретического тура 120 минут.

Выполнение теоретических заданий целесообразно организовать следующим образом:

- не спеша, внимательно прочитайте задание и определите, наиболее верный и полный ответ;

- отвечая на тестовые задания определите, какой из предложенных вариантов наиболее верный и полный и обведите (напишите) букву, соответствующую выбранному Вами ответу;

- отвечая на теоретический вопрос, обдумайте и сформулируйте конкретный ответ только на поставленный вопрос;

- если Вы выполняете задание, связанное с заполнением таблицы или схемы, не старайтесь детализировать информацию, вписывайте только те сведения или данные, которые указаны в вопросе;

- после выполнения всех предложенных заданий еще раз удостоверьтесь в правильности Ваших ответов;

- если потребуется корректировка выбранного Вами варианта ответа, то неправильный вариант ответа зачеркните крестиком, и рядом напишите новый.

Задание теоретического тура считается выполненным, если Вы вовремя сдаете его членам жюри. Задания общей части с 1 по 5 оцениваются максимально в 2 балла. Задания специальной части с 6 по 10 оцениваются максимально в 2 балла, с 11 по 20 оцениваются максимально в 3 балла. Творческое задание оценивается максимально в 10 баллов. Итоговая максимальная оценка 60 баллов.

Общая часть

Задание 1. (2 балла)
Какие из перечисленных видов автоматизации применяются в промышленности?

A. Роботизация
B. Компьютерное управление
C. 3D-печать
D. Искусственный интеллект
E. Цифровые двойники

Задание 2. (2 балла)
Какие из перечисленных мер относятся к техническим средствам защиты информации?

A. Антивирусные программы
B. Брандмауэры
C. Системы обнаружения вторжений
D. Шифрование данных
E. Пароли

Задание 3. (2 балла)
Какой из перечисленных принципов является основополагающим в промышленном дизайне?

A. Функциональность
B. Эстетика
C. Эргономика
D. Экологичность

Задание 4. (2 балла) Решите задачу
Соотнесите типы 3D-моделирования с их основными особенностями.

Типы 3D-моделирования	**Описание**
1) Полигональное моделирование	A. Использование математических кривых для создания гладких поверхностей
2) NURBS-моделирование	B. Создание моделей из отдельных геометрических примитивов
3) Voxel-моделирование	C. Моделирование объектов путем деления пространства на кубические элементы
4) Процедурное моделирование	D. Моделирование с использованием алгоритмов и математических формул

Задание 5. (2 балла)
Установите правильную последовательность этапов создания прототипа:

A. Тестирование прототипа
B. Выбор материалов и инструментов
C. Разработка концепции прототипа
D. Определение функциональных требований
E. Сборка прототипа

Специальная часть

Задание 6. (2 балла)
Продолжите предложение: «Учетная запись пользователя – это……»

A. совокупность следующей информации о пользователе: фамилия, имя, пароль, дата рождения
B. уникальная информация, позволяющая различить пользователей
C. секретная информация, известная только пользователю или системе, используемая для прохождения аутентификации
D. совокупность информации о пользователе: идентификатор, пароль, некоторая дополнительной информация

_____

Задание 7. (2 балла)
Выделяют несколько степеней надежности Интернет-ресурса: 1 степень – надежный; 2 степень – достаточно надежный; 3 степень – вызывает подозрение; 4 степень – не заслуживает доверия.
Выберите из предложенных характеристик ресурса, те из них, которые могут свидетельствовать <u>только о четвертой</u> степени надежности.

A. Определяется авторство ресурса
B. Указаны контакты авторов
C. Очевидна аккуратность ресурса
D. Присутствует адрес ресурса
E. Обозначена цель ресурса
F. Наличие актуальных данных
G. Указаны источники информации

_____

Задание 8. (2 балла)
В фразе «кротовые пенаты злейшие козни сада» спрятана некая информация. Она может быть получена в переменной result с помощью программы, фрагмент которой приведен ниже. **Найдите спрятанную информацию**.

```
int const N=5;
string s[N], result="";
s[0]="кротовые";   s[1]="пенаты";   s[2]="злейшие";   s[3]="козни";   s[4]="сада";
for(int i=0;i<N;i++)
        result=result+s[i][3];
cout << "result=" <<result;
```

Задание 9. (2 балла)

Два приятеля договорились поиграть в сети. В процессе игры приятели поссорились. Один из них перешел на оскорбления с использованием ненормативной лексики.

Проанализируйте данную ситуацию, и ответьте на следующие вопросы:

1). Какими законами регулируется оскорбление в сети?

A. Гражданским кодексом Российской Федерации» (ГК РФ)

B. Уголовным кодексом Российской Федерации» (УК РФ)

C. Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

---

2) Куда можно обращаться в случае оскорбления в сети

A. В суд о возмещении морального ущерба B. к администратору сайта

C. к модератору игры с просьбой об исключении обидчика из игрового сообщества

Задание 10. (2 балла)

Какие из перечисленных документов свидетельствуют о лицензированном ПО?

A. Сертификат подлинности.

B. При поставке коробочной версии на коробке присутствуют брендовые голограммы, наклейки

C. Договор с конечным пользователем

D. Руководство пользователя. Есть не во всех случаях.

E. Руководство администратора

F. Документация, приложенная к продукту.

Задание 11. (3 балла)

Текст зашифровали последовательно с помощью двух таблиц перестановок 4*6 и 8*3 (строка*столбец). Ниже дан шифрованный текст. **Какой был исходный текст?**

конилиявивднриспацапаофь

Задание 12. (3 балла)

Целостность информации – важная составляющая информационной безопасности. В процессе выполнения программы информация может искажаться за счет переполнения типов. Пусть для переменной целого типа данных в памяти компьютера выделено 1 байт памяти, и ее значения могут лежать в диапазоне от 0 до 255. **Какое значение будет в этой переменной, если ей присвоить значение 98 и прибавить 254?**

_____

Задание 13. (3 балла)

Четырем новым сотрудникам лаборатории были выданы временные пароли.

Определите, кому из сотрудников достался самый не надежный пароль.

Временные пароли:

Первому сотруднику - A4$Fz

Второму сотруднику - 5A3GZ

Третьему сотруднику - 7BZ6s4q

Четвертому сотруднику - 1gG9B1$

Первому и четвертому сотрудникам пароли выдали на трое суток, второму и третьему - на двое суток.

Пароли полностью состоят из всех символов алфавита. Строчные и прописные буквы считаются разными символами.

Например, пароли 1W2r3 и 3E8r1 записаны с помощью алфавита: 1, W, 2,r,3,8,E

Известно:

- вероятность подбора пароля определяется по следующей формуле:

$$P = (V \cdot T) / A^L \text{ , где}$$

A – символы, входящие в пароль (символы алфавита, из которых составлены пароли);

L – количество символов в пароле;

T – максимальный срок действия пароля;

V– скорость перебора паролей злоумышленником (количество паролей в минуту);

- злоумышленники используют технические средства подбора паролей, которые обеспечивают скорость перебора 30 паролей в минуту.

_____

Задание 14. (3 балла)

Поточный шифр Виженера заключается в том, что буква исходного текста заменяется на другую не только в зависимости от того, какая эта буква, но и от того, на каком месте она стоит. То есть, к коду буквы текста добавляется код буквы ключа по модулю мощности

алфавита. Ниже представлен алфавит с кодами букв, шифрованный текст и ключ. **Найдите исходный текст.**

буква	код	е	5
а	0	ж	6
б	1	з	7
в	2	и	8
г	3	к	9
д	4	л	10

е в ж з г а – шифротекст

к а б а л а – ключ

_____

Задание 15. (3 балла)

Алиса посылает Бобу сообщение и ставит в конце подпись. Сообщение Алиса шифрует (обозначим функцию шифрования как *f*) открытым ключом Боба (*Кев*). Только Боб может расшифровать его, так как он знает закрытый ключ – ключ расшифрования. В качестве подписи Алиса использует собственное имя, шифруя его своим закрытым ключом(*Kda*). Только Алиса может зашифровать подпись таким ключом, так как только она его знает.

В результате получилось зашифрованное сообщение с присоединенной подписью

f_{keb}(Дай Еве две конфеты) f_{kda}(Алиса)

Какие проблемы могут возникнуть при использовании такой схемы шифрования и подписи?

_____

_____

_____

_____

_____

Задание 16. (3 балла)

О чём говорит вывод команды данной утилиты? Обратите внимание на описание строк.

```
$ binwalk 123.jpg | grep -v 'Unix path'
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.02
46            0x2E            TIFF image data, big-endian, offset of first image
directory: 8
628320        0x99660         Zip archive data, at least v2.0 to extract, compressed size:
21, uncompressed size: 19, name: input.txt
628471        0x996F7         End of Zip archive
628493        0x9970D         PNG image, 385 x 338, 8-bit/color RGBA, non-interlaced
628584        0x99768         Zlib compressed data, compressed
```

A. Файл является картинкой в формате JPG

B. Файл является картинкой в формате PNG
C. Файл является склейкой из двух файлов различных типов данных
D. Файл является ZIP-архивом

Задание 17. (3 балла, по 1 баллу за пункт ответа)

Задача на расследование инцидентов (форензика).

Компьютерная форензика — это область, связанная с расследованием преступлений и сбором доказательств из цифровых устройств. Важно не только собирать данные и восстанавливать информацию, но и понимать, какие права доступа имеют различные пользователи к этим данным. Это знание может помочь установить, кто мог получить доступ к какой информации и в какой момент времени.

Задание:

Представьте, что произошло преступление: кто-то незаконно удалил важные данные с компьютера в офисе. Ваша задача — помочь следователям восстановить информацию, понять права доступа и установить порядок действий в ходе расследования.

Исходные данные:

В ходе расследования была найдена файловая система компьютера с информацией о файлах и правах доступа к ним. Файлы представлены в виде таблицы:

Имя файла	Тип данных	Размер (КБ)	Дата создания	Дата изменения	Удалён (Да/Нет)	Права доступа
report.docx	Документ	150	2024-10-01	2024-10-05	Нет	Чтение, Запись: Админ
photo.jpg	Изображение	200	2024-09-15	2024-09-20	Да	Чтение: Все, Запись: Админ
notes.txt	Текстовый файл	50	2024-10-02	2024-10-03	Нет	Чтение, Запись: Пользователь
secret_data.xlsx	Электронная таблица	300	2024-09-29	2024-10-01	Да	Чтение, Запись: Админ
backup.zip	Архив	500	2024-10-05	2024-10-05	Нет	Чтение: Все, Запись: Админ

Ответьте на следующие вопросы:

a) Сколько файлов было удалено? Укажите имена файлов.

---

b) Какой файл имеет наибольший размер? Укажите имя файла и его размер.

---

c) Определите, кто мог удалить файл photo.jpg, основываясь на правах доступа?

Задание 18. (3 балла)

Восстановление удалённых файлов

У вас имеется утилита для восстановления удалённых данных. Программа имеет возможность сканировать текущее состояние диска, и если не было совершено преднамеренного затирания данных, то файлы можно попробовать восстановить.

Предположим, что восстановление файла занимает определённое время (в секундах) в зависимости от его размера:

- 1 КБ — 0,1 секунды
- 1 МБ — 5 секунд

Вычислите, сколько времени потребуется для восстановления всех удалённых файлов из предыдущего пункта заданий (в секундах).

Задание 19. (3 балла)

Регулярные выражения (regex) используются для поиска и выполнения операций над строками в соответствии с определёнными шаблонами. Вот некоторые основные правила:

1. `.` — соответствует любому одиночному символу, кроме символа новой строки.
2. `*` — соответствует нулю или более повторениям предыдущего элемента.
3. `+` — соответствует одному или более повторениям предыдущего элемента.
4. `?` — соответствует нулю или одному повторению предыдущего элемента.
5. `^` — соответствует началу строки.
6. `$` — соответствует концу строки.
7. `[abc]` — соответствует любому из символов a, b или c.
8. `\d` — соответствует любой цифре (эквивалент [0-9]).
9. `\w` — соответствует любому алфавитно-цифровому символу (эквивалент [a-zA-Z0-9_]).
10. `{n}` — соответствует ровно n повторениям предыдущего элемента.

Выберите регулярное выражение для поиска телефонных номеров в формате `(XXX) XXX-XXXX`, где `X` — любая цифра. Например, `(123) 456-7890` соответствует шаблону.

A. `r'\(\d{3}\) \d{3}-\d{4}'`
B. `r'\d{3}-\d{3}-\d{4}'`
C. `r'\(\d{2,3}\) \d{3}-\d{4,5}'`

Задание 20. (3 балла)

Искусственный интеллект и составление Prompt-запросов.

Задача состоит в создании prompt-запроса для туристического искусственного интеллекта, который должен учитывать различные аспекты пожеланий клиентов турагентства. *Запрос должен:*

1. Учитывать предпочтения пользователя к климату (жаркий, прохладный, умеренный).
2. Включать интересы пользователя к активности (пляжный отдых, культурные мероприятия, активные путешествия).
3. Указывать желаемую продолжительность путешествия (1 неделя, 2 недели).
4. Запрашивать бюджет пользователя (низкий, средний, высокий).

Выберите один из следующих вариантов, который наиболее точно соответствует всем требованиям:

A. "Расскажи о лучших местах для путешествий."
B. "Помоги мне спланировать путешествие, учитывая мои предпочтения: мне нужен жаркий климат, интересуют пляжный отдых, на 2 недели, с высоким бюджетом."
C. "Предложи места для путешествия в прохладные страны, интересует обширная культурная программа, активные путешествия. Бюджет средний."
D. "Какие ты можешь посоветовать актуальные предложения для отдыха?"

Задание 21. (10 баллов)

Задание повышенной сложности

Введение в теорию для понимания алгоритма шифрования RSA и его принципов.

RSA (Rivest-Shamir-Adleman) — это один из первых и самых известных алгоритмов шифрования с открытым ключом. Он широко используется для обеспечения безопасности данных при передаче по сети. Принципы работы RSA основываются на простых числах и их свойствах. В отличие от симметричного шифрования, где используется один и тот же ключ для шифрования и дешифрования, в RSA используются два ключа: открытый (который можно свободно распространять) и закрытый (который должен храниться в секрете). Таким образом зашифровать сообщение могут многие, а расшифровать только обладатель закрытого ключа.

Основные шаги алгоритма RSA:

1. **Выбор простых чисел (p) и (q)**
   Два различных простых числа.
2. **Вычисление (n)**
   (n = p q). Получив простые числа p, q, надо их перемножить.
3. **Вычисление функции Эйлера (φ (n))**
   Для двух простых чисел вычисляется так: $\varphi(n) = (p-1)(q-1)$.
4. **Выбор открытого ключа (e)**
   Целое число, которое должно быть взаимно простым с ($\varphi(n)$). Это должно быть такое число, которое бы попало в следующий диапазон: $1 < e < \varphi(n)$.

При этом, его наибольший общий делитель (НОД) должен быть равен 1, или, другими словами, чтобы ни одно целое число, кроме 1, не смогло поделить e и φ(n), то есть, чтобы у этих двух чисел не было наибольшего общего делителя, больше чем 1.

Примеры:

- Числа 5 и 15 имеют НОД(5,15) = 5 — число 15 делится на 5, и 5 делится на 5 без остатка
- НОД(7, 14) = 7 — число 7 делится на 7, и 14 делится на 7 тоже
- НОД(12, 15) = 3 — число 12 делится на 3, число 15 делится на 3
- НОД(9, 11) = 1 — вот это в самый раз, ни одно число не делится, кроме как на 1

5. **Вычисление закрытого ключа (d)**
   Инверсия (e) по модулю (φ(n)), выглядит это так: $d = e^{-1} \ mod \ \varphi(n)$
   Но её можно упростить до: $(de) \ mod \ \varphi(n) = 1$

Задание:

Часть 1: Понимание основ

1. **Выбор простых чисел. (1 балл)**

   Выберите пару чисел, с которыми вы бы могли выполнять операции

   - (p = 7), (q = 13)
   - (p = 9), (q = 11)
2. **Вопрос (1 балл):** Почему важно, чтобы (p) и (q) были простыми числами? Объясните, какие последствия будут, если одно из выбранных чисел не является простым.

Часть 2: Вопросы на понимание

3. **Генерация ключей (2 балла):**
   Используя значения выбранные в части 1 (p и q):
   - Вычислите (n)
   - Вычислите (φ(n))

4. **Выбор открытого ключа (2 балла):**
   Какое значение вы могли бы выбрать для (e), если (φ(n) = 72)? Как вы можете это обосновать?

5. **Закрытый ключ (1 балл):**
   Почему важно, чтобы закрытый ключ (d) не был известен всем? Опишите, как вы могли бы использовать (d) для дешифрования.

Дополнительные вопросы

6. **Преимущества RSA (1 балл):**
   Объясните, почему алгоритм RSA считается безопасным для передачи данных.
7. **Применение RSA (1 балл):**
   В каких ситуациях вы можете использовать RSA в реальной жизни? Приведите пример.
8. **Дополнительные примеры (1 балл):**
   Приведите ещё один пример простых чисел ((p, q)) и объясните, что произойдет, если бы вы использовали их вместо тех, которые выбрали.