

## ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ

## МУНИЦИПАЛЬНЫЙ ЭТАП

## Профиль

## «Информационная безопасность»

## ПРАКТИЧЕСКИЙ ТУР

Возрастная группа – 7-8-е классы

**Задание 1. Решение задачи простоты**

Профессор математики Гэри Селдон в своих изысканиях науки «психоистории» столкнулся с непростой задачей. Камнем преткновения его работы стал вопрос по нахождению простых чисел. Найти то он их нашел, а вот проверить что оно простое было сложно. Для таких Юных ребят как вы это дело на пять минут.

Для решения задачи нужно написать программу, которая проверит число что оно делится только на себя и на 1 и других делителей нету.

**Решение**

```
def Prime(n):
```

```
    d = 2
```

```
    while n % d != 0:
```

```
        d += 1
```

```
    return d == n
```

Правильны ответы:

- 1) 13
- 2) 3
- 3) 7
- 4) 5
- 5) 67

В той последовательности как это должно быть.

## Задание 2. Поиск простых чисел из диапазона чисел

Профессору математики Гэри Селдон опять нужна Ваша помощь. Он проверил все нужные числа на простоту, но он осознал, что не все простые числа он учел и где-то потерял исходную информацию. Гэри просит Вас вновь помочь ему и вывести все простые числа 950 до 1001.

Данное решение, более расширенное так, как надо найти в множестве решений. Но решается так же только нужно добавить генератор, который будет проверять числа на простоту.

```
def Prime(n):  
    d = 2  
    while n % d != 0:  
        d += 1  
    return d == n  
for I in range(950,1001):  
    print(Prime(i))
```

Ответ по задаче.

```
953  
967  
971  
977  
983  
991  
997  
1001
```

## Задание 3. Дешифровка сообщения

Случилось страшное Империя нападает на Академию и нам срочно нужно обеспечить безопасность наивысшего уровня. Вам как самому разбирающемуся в теме безопасности поручили спасти академию и помочь сохранить секреты. Главная проблема — пароль от системы который забыли. Пароль хранился в маленькой красной записной книжечке в зашифрованном виде, но программу дешифрования потеряли – она сломалась. По секрету Вам сказали, что использовался шифр цезаря для алфавита. Шифр текст «Тгусоя ахс рз хсоянс прсёс дцне, рс л еюфснгв архустлв»

Решение:

Данная задача решается не классическим алгоритмом цезаря так как ключ динамический не равный 3. Требуется реализовать поиск ключа и получить читаемый текст. Смещение ключа ROT30:

```

alfavit =
'АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬ
ЭЮЯ абвгдеёжзийклмнопрстуфхцчшщъыьэюяабвгдеёжзийклмнопрстуфхцчшщъыьэюя '
smeshenie = int(input('Шаг шифровки: '))
message = input("Сообщение для Дешифровки: ").upper()
itog = ""
lang = input('Выберите язык RU/EU: ')
if lang == 'RU':
    for i in message:
        mesto = alfavit.find(i)
        new_mesto = mesto + smeshenie
        if i in alfavit_RU:
            itog += alfavit[new_mesto]
        else:
            itog += i
print (itog)

```

**Ответ:**

Пароль это не только много букв, но и высокая энтропия

#### **Задание 4. Секретное сообщение**

На Терминусе в Академии все были очень умные и для общения между собой кроме естественного языка использовали сообщения специально обработанные каким-то алгоритмов шифрования. Все понимали друг друга, но вы как молодой исследователь столкнулись с трудностями по понимаю передаваемых сообщений. Для этих целей нужно написать программу, которая позволяет, получает исходную строку от пользователей с клавиатуры и расшифровывает строку со всем возможными вариантами, известно, что каждое сообщение начинается со слова «Привет». Расшифруйте диалог двух людей и выведите на экран сообщение на естественном языке.

**Решение**

Данная задача решается не классическим алгоритмом цезаря так как ключ динамический не равный 3. Требуется реализовать поиск ключа и получить читаемый текст.

```

alfavit =
'АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬ
ЭЮЯ абвгдеёжзийклмнопрстуфхцчшщъыьэюяабвгдеёжзийклмнопрстуфхцчшщъыьэюя '
smeshenie = int(input('Шаг шифровки: '))
message = input("Сообщение для Дешифровки: ").upper()
itog = ""
lang = input('Выберите язык RU/EU: ')
if lang == 'RU':
    for i in message:
        mesto = alfavit.find(i)
        new_mesto = mesto + smeshenie
        if i in alfavit_RU:
            itog += alfavit[new_mesto]
        else:
            itog += i

```

```
print (itog)
```

Привет, друг

Привет, как твои дела

Привет, дела отлично вот думаю когда наступит новый переломный момент

Привет, Гэри говорил что скоро, надо сходит в пещеру может уже появилось новое пророчество

Привет, Пошли посмотрим

## Задание 5. Таинственное устройство

В пещере Академии, где Гэри вещал разрешение вопросов переломных моментов для Академии были найдены странные цифры и машину, требующую ввода двух простых чисел. Ученые ломают голову что в этом послание скрыто. Вы предположили, что Гэри Селдон увлекался криптографией и использовал Алгоритм Блюм – Блюм – Шуба « $X_{i+1} = X_i^2 \bmod m$ » в своих посланиях, где  $m = p * q$  – является произведением двух больших простых  $p$  и  $q$ . Важно, что  $p$  и  $q$  должны давать при деление на 4 одинаковый остаток, например 3. Вы вызвались написать программу, которая найдет числа, которые использовались для генерации гаммы. Число, написанное на стене 130.

Решение:

Требуется реализовать алгоритм и подобрать такие два числа что бы на шестом шагу генерации гаммы ответом было 130.

```
x = 0
```

```
y = 0
```

```
x = int(input("Number p= "))
```

```
y = int(input("Number q= "))
```

```
m = x*y
```

```
x = x%4
```

```
y = y%4
```

```
print(m)
```

```
if x==y:
```

```
    for i in range(6):
```

```
        b=(x**2)%m
```

```
        print(b)
```

```
        x=b
```

```
else:
```

```
    print("bye")
```

Ответ:

Два числа используемые в задаче 7 и 19

Гамма

Шаг1 - 9

Шаг2 - 81

Шаг3 - 44

Шаг4 - 74

Шаг5 - 23

Шаг6 - 130

## Задание 6. Криптографические шифры

Академия очень интересовалась переговорами Империи и хотела знать, о чем они говорили, алфавит сообщений использует только заглавные буквы. При выполнении различных манипуляций было выяснено, что Империя использует гамму из чисел Фибоначчи. Вам, как зарекомендовавшему себя специалисту информационной безопасности, поручили проанализировать перехваченный текст и написать программу, которая будет выполнять дешифрование сообщения. Программа получает сообщение с клавиатуры, проводит вычисления и выводит на экран открытый текст. Для определения выполненного задания точно известно, что в конце передачи передается слово подтверждение «береза».

Решение:

Задача направлена на формирование последовательности чисел Фибоначчи, формирования алфавита и выполнение операции сложения по модулю 33. Ключевое это слово береза как ориентир на получения искомого результата. Для решения требуется написать программный код.

```
def fiban(n):
```

```
    fib1 = 1
```

```
    fib2 = 1
```

```
    n = int(n)
```

```
    i = 0
```

```
    while i < n - 2:
```

```
        fib_sum = fib1 + fib2
```

```
        fib1 = fib2
```

```
        fib2 = fib_sum
```

```
        i = i + 1
```

```
        k.append(fib2%33)
```

```
n = input('Номер элемента ряда Фибоначчи: ')
```

```
fiban(n)
```

```
buk = ['A', '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']
```

```
b=0
```

```
for i in buk:
```

```
    b+=1
```

```
print(b)
```

```
print(k)
```

```
str = input('enter')
```

```

r=[]
for i in str:
    c=0
    for m in buk:
        c+=1
        if i==m:
            r.append(c)
            break
    else:
        pass

print(r)
l=[]
z=[]
q=[]
for i in range(0,len(r)):
    l.append((r[i]+k[i])%33)
    q.append(buk[l[i]-1])
print(l)
print("".join(q))
for i in range(len(r)):
    z.append((l[i]-k[i])%33)
print(z)

```

Ответ:

МЫНАШЛИАКАДЕМИЮБЕРЕЗА

## Примерные критерии оценки проектного тура

| Критерии оценки проекта         |       |                                                                                                                                                                                                                                                                               | Баллы |
|---------------------------------|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Пояснительная записка 10 баллов | 1     | Содержание и оформление документации проекта                                                                                                                                                                                                                                  | 7     |
|                                 | 1.1   | Общее оформление: (ориентация на ГОСТ 7.32-2017 Международный стандарт оформления проектной документации) (да – 1; нет – 0)                                                                                                                                                   | 1     |
|                                 | 1.2   | Качество теоретического исследования                                                                                                                                                                                                                                          | 2     |
|                                 | 1.2.1 | Наличие актуальности и обоснование проблемы в исследуемой сфере.. (да – 0,5; нет – 0)                                                                                                                                                                                         | 0/0,5 |
|                                 | 1.2.2 | Формулировка темы, целей и задач проекта (сформулированы полностью – 0,5; нет полной формулировки – 0)                                                                                                                                                                        | 0/0,5 |
|                                 | 1.2.3 | Сбор информации по проблеме (оценка распространенности проблемы, наличия запроса потенциальных пользователей на средство ее решения, описание пользовательской аудитории) (да – 0,5; нет – 0)                                                                                 | 0/0,5 |
|                                 | 1.2.4 | Предпроектное исследование: анализ наличия прототипов                                                                                                                                                                                                                         | 0/0,5 |
|                                 |       | и аналогов (да – 0,5; нет – 0)                                                                                                                                                                                                                                                |       |
|                                 | 1.2.5 | Предложения решения выявленной проблемы. Авторская концепция проекта. Выбор оптимальной идеи. Описание проектируемого решения выявленной проблемы (да – 0,5; нет – 0)                                                                                                         | 0/0,5 |
|                                 | 1.3   | Креативность и новизна проекта                                                                                                                                                                                                                                                | 2     |
|                                 | 1.3.1 | Оригинальность предложенных идей:<br>– отсутствие известных прямых аналогов предложенного решения;<br>– соответствие современным представлениям о решениях подобного класса, требованиям к ним;<br>– потенциальное удобство применения для пользователя;<br>(да – 1; нет – 0) | 0/1   |

|                                       |       |                                                                                                                                                                                                                                                                                                                                                                                                                |         |
|---------------------------------------|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                       | 1.3.2 | Значимость и корректность проекта (проект направлен на разработку конкретного применимого продукта, повышающего уровень безопасности пользователей информационных систем путем решения конкретной проблемы информационной безопасности);<br>(да – 2; опосредованно/решением общей или смежной проблемы – 1; нет/не направлен на решение конкретной проблемы/не направлен на создание конкретного продукта – 0) | 0/0,5/1 |
|                                       | 1.4   | Разработка технологического процесса                                                                                                                                                                                                                                                                                                                                                                           | 2       |
|                                       | 1.4.1 | Выбор технологии реализации, формы итогового решения и инструментария его получения (аппаратного, программного или теоретического)<br>(есть ссылки или описание – 0,5, нет – 0)                                                                                                                                                                                                                                | 0/0,5   |
|                                       | 1.4.2 | Качество представления ожидаемого результата, его специализированных (связанных с решением задачи информационной безопасности) и пользовательских (удобство, простота использования и т. п.) свойств (уровень графической подачи с использованием компьютерных программ или от руки, соответствие чертежей ГОСТ)<br>(да – 0,5; нет – 0)                                                                        | 0/0,5   |
|                                       | 1.4.3 | Оценка потенциала применения результата проекта; предложения по внедрению<br>(проект будет полезен широкому кругу пользователей – 1; продукт имеет ограниченное применение – 0,5; явного потенциала внедрения нет – 0)                                                                                                                                                                                         | 0/0,5/1 |
| Оценка планируемого изделия 15 баллов | 2     | Дизайн продукта творческого проекта                                                                                                                                                                                                                                                                                                                                                                            | 15      |
|                                       | 2.1   | Новизна и оригинальность продукта, его соответствие отраслевым тенденциям и требованиям к продуктам такого класса<br>(Объект новый – 4; оригинальный – 2, стереотипный – 0)                                                                                                                                                                                                                                    | 0/2/4   |
|                                       | 2.2   | Композиция проектируемого объекта<br>(сочетание свойств, направленных на решение выявленной проблемы с потенциалом для применения, удобством использования, универсальностью, пригодностью для использования в широком спектре информационных систем)<br>(целостность – 2; не сбалансированность – 0)                                                                                                          | 0-2     |
|                                       | 2.3   | Планируемый состав представляемых результатов, сопроводительных документов и материалов<br>(исчерпывающе для внедрения – 3, требуется дополнение состава материалов для облегчения использования или внедрения/продукт предназначен только для специалистов в узкой области – 2, заявляемый состав материалов недостаточен для использования – 0)                                                              | 0/1/3   |

|                                 |     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |
|---------------------------------|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                 | 2.4 | <p>Рациональный выбор потребности и трудоёмкости создания продукта, сложность; многофункциональность и вариативность демонстрируемого результата;<br/>(от 0 до 3 баллов)</p> <p>Продукт рационально сложен при заявленном функционале и запросе на его внедрение (просто или умеренно сложно создать, нужно широкому кругу пользователей) – 3 балла;</p> <p>Продукт излишне сложен при ограниченном функционале или ограниченной потребности в нем (сложно создавать, нужен ограниченному кругу пользователей) – 1,5 балла</p> <p>Продукт излишне сложен при ограниченной или не продемонстрированной явно потребности в нем (очень сложно/трудоемко создавать при недостаточной для такого уровня сложности потребности или продукт создается для демонстрации принципиальной возможности без явной потребности в нем) – 0 баллов</p> | 0-3   |
|                                 | 2.5 | <p>Перспективность и конкурентоспособность спроектированного продукта (наличие ближайших конкурентов, запроса от пользовательского сообщества, конкретных пользователей – юридических лиц) (от 0 до 3 баллов) Продукт адресован широкому кругу пользователей – 3 балла;</p> <p>Продукт адресован широкому кругу пользователей, но не решает конкретной проблемы – 2 балла;</p> <p>Продукт адресован ограниченной группе специалистов/конкретной организации – 1 балл;</p> <p>Продукт не имеет явного запроса от пользовательского сообщества на его создание – 0 баллов</p>                                                                                                                                                                                                                                                            | 0-3   |
|                                 | 3   | Процедура презентации проекта                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 8     |
| Оценка защиты проекта 10 баллов | 3.1 | <p>Регламент презентации (от 0 до 2 баллов)</p> <p>Соблюдение временного регламента, заявленного организаторами (соблюдение без превышения – 0,5 балл, превышение регламента – 0 баллов);</p> <p>Соответствие ожидаемому уровню делового этикета и имиджа участника (полное соответствие – 0,5 балл, неполное соответствие – 0 баллов)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 0/1   |
|                                 | 3.2 | <p>Качество подачи материала и представления изделия: - оригинальность представления и качество электронной презентации (1балл);</p> <p>- культура речи, четкость, конкретность и логика изложения проблемы исследования (0,5 балл);</p> <p>владение понятийным профессиональным аппаратом (0,5 балл)</p> <p>(от 0 до 2 баллов)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 0 – 2 |

|  |     |                                                                                                                                                                                                                                                                                                                                                                                             |       |
|--|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|  | 3.3 | Понимание основных принципов в соответствующей области информационной безопасности<br>- Полное соответствие позиции автора и предлагаемых объяснений основным принципам информационной безопасности, сформулированным в настоящее время (1 балл);<br>Опора на научные или аналитические публикации последних 3-5 лет при аргументации положений проекта (1 балл);<br><br>(от 0 до 2 баллов) | 0/1/2 |
|  | 3.4 | Понимание сути задаваемых вопросов и аргументированность ответов<br><br>(от 0 до 2 баллов)                                                                                                                                                                                                                                                                                                  | 0/1/2 |
|  | 3.5 | Соответствие содержания выводов содержанию цели и задач, конкретность и самостоятельность выводов (соответствует полностью – 1; не соответствует - 0)                                                                                                                                                                                                                                       | 0/1   |
|  |     | Итого                                                                                                                                                                                                                                                                                                                                                                                       | 30    |

## CTF

Олимпиада состоит из 6 заданий по темам

- Реверс (анализ исходных текстов компьютерных программ)
- Web (поиск уязвимостей web-приложений)
- Forensics (поиск следов инцидентов информационной безопасности)
- Linux\Unix (Misc) (задания смешанной категории, защита ОС Linux\Unix)
- Анализ трафика
- Средства защиты информации (СЗИ).

Каждый решение оценивается в 7 баллов. (Да/Нет) Найденные флаги вводятся на Платформе. Количество попыток ввода флага не ограничено. За ошибочно введенный флаг баллы не снижаются. Максимальное количество баллов 42.