ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТРУДУ (ТЕХНОЛОГИИ)

МУНИЦИПАЛЬНЫЙ ЭТАП —ТЕОРЕТИЧЕСКИЙ ТУР

2024-2025 учебный год

Профиль «Информационная безопасность» — 10-11 классы

Уважаемый участник олимпиады!

Вам предстоит выполнить теоретические и тестовые задания.

Время выполнения заданий теоретического тура 2 академических часа (120 минут).

Выполнение тестовых заданий целесообразно организовать следующим образом:

– не спеша, внимательно прочитайте тестовое задание;

– обратите внимание, что задания, в которых варианты ответа являются продолжением текста задания, предполагают единственный ответ; задания, в которых имеется инструкция «укажите все», предполагает несколько верных ответов;

– определите, какой (или какие) из предложенных вариантов ответа наиболее верный и полный; другие варианты ответа могут быть частично верными, верными, но неточными или неполными, верными без учета условий конкретного задания – такие ответы признаются неверными при наличии более точного, полного или учитывающего условия варианта;

– напишите букву (или набор букв), соответствующую выбранному Вами ответу;

– продолжайте таким образом работу до завершения выполнения тестовых заданий;

– 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.

Выполнение теоретических (письменных, творческих) заданий целесообразно организовать следующим образом:

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

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

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

– после выполнения всех предложенных заданий еще раз удостоверьтесь в правильности выбранных Вами ответов и решений.

Предупреждаем Вас, что:

– при оценке тестовых заданий, где необходимо определить один правильный ответ, 0 баллов выставляется за неверный ответ и в случае, если участником отмечены несколько ответов (в том числе правильный), или все ответы;

– при оценке тестовых заданий, где необходимо определить все правильные ответы, 0 баллов выставляется, если участником отмечены неверные ответы, большее количество ответов, чем предусмотрено в задании (в том числе правильные ответы) или все ответы.

Задания теоретического тура считается выполненными, если Вы вовремя сдаете бланк ответов членам жюри. Максимальная оценка – 100 баллов).

ОБЩАЯ ЧАСТЬ

1. Приведите, используя условный графический пример, как на чертежах изображаются сечение и разрез. По вашему примеру должно быть понятно, чем они отличаются.

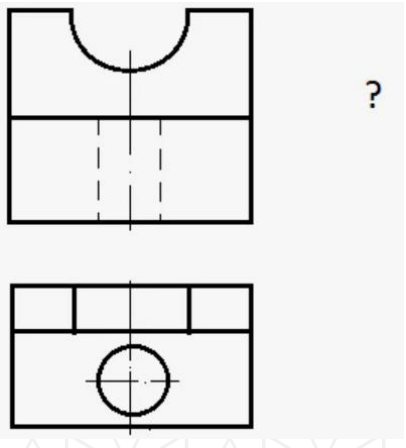
2. В жилой комнате площадью 16 м2 после ремонта устанавливают новое освещение. Посчитайте (основываясь на данные таблицы), какой должна быть минимальная потребляемая мощность (Вт) одной светодиодной лампы в 3-х рожковой люстре, чтобы люстра могла обеспечить помещение нормой освещенности согласно СНиП 150 Лк на 1 м2.

Люмен	250	450	800	1100	1600
Потребляемая мощность светодиодной лампы	4 Вт	6 Вт	9 Вт	12 Вт	15 Вт

3. Установите правильное соответствие

I. Доходы	А Нехватка чего-либо, превышение расходов над доходами
II. Бюджет	Б Денежные затраты на покупку различных товаров и услуг
III. Баланс	В Смета доходов и расходов на определенный срок
IV. Расходы	Г Сумма всех поступлений денежных средств бюджет семьи за определенный период
V. Дефицит	Д Равновесие между доходами и расходами

4. По двум видам (главному виду и виду сверху) построить вид слева.



5. Используя метод фокальных объектов, предложите идею создания предмета интерьера офисного помещения. (В этом задании необходимо показать, как вы используете метод фокальных объектов - оценивается именно эта способность)

СПЕЦИАЛЬНАЯ ЧАСТЬ

Билл устраивается на работу в “ООО Гравити”, организацию, которая занимается кибербезопасностью. Проходя собеседование, он сильно разволновался, и ему явно нужна помощь. Помогите Биллу вспомнить основы информационной безопасности. В этом блоке на каждый вопрос может быть более одного верного варианта ответа.

6. Что такое "симметричное шифрование"?

а) Метод шифрования, при котором для шифрования и расшифровки используется один и тот же ключ

б) Метод шифрования, при котором используется два разных ключа для шифрования и расшифровки

в) Метод, при котором шифруются только числовые данные, а текст остаётся открытым

г) Метод шифрования, который использует алгоритм на основе случайных чисел

7. Какой из типов атак называется "атака с перебором" (brute-force)?

а) Атака, при которой злоумышленник пытается подобрать правильный пароль или ключ, перебирая все возможные варианты

б) Атака, при которой перехватываются данные, передаваемые между устройствами

в) Атака, при которой происходит взлом пароля через уязвимость в сети

г) Атака, при которой используется поддельный сертификат для подключения к серверу

8. Что такое "SQL-инъекция" и как она может угрожать безопасности веб-приложений?

а) Атака, при которой данные, передаваемые через SQL-запросы, подменяются в процессе передачи

б) Атака, при которой сервер не может обрабатывать запросы от клиентов, так как они перегружают его ресурсами

в) Атака, при которой пользовательский ввод использует неподобающие символы для обхода защиты

г) Атака, при которой злоумышленник вводит вредоносный SQL-код в поле ввода, чтобы получить несанкционированный доступ к базе данных

9. Какие из следующих утверждений о криптографических протоколах и алгоритмах верны? (Выберите все верные ответы.)

а) Протокол SSL/TLS используется для шифрования данных в сети, но из-за устаревших версий SSL он больше не является безопасным

б) Алгоритмы асимметричного шифрования (например, RSA) считаются более быстрыми и эффективными, чем симметричные (например, AES) при защите

больших объёмов данных
в) Алгоритм RSA используется для шифрования больших объёмов данных, но для передачи ключей для симметричного шифрования он подходит лучше
г) Хэш-функции, такие как SHA-256, могут быть использованы для защиты паролей, так как они необратимы и не позволяют восстановить исходные данные

Благодаря вашей помощи Билл смог устроиться на работу. Первой его задачей станет защита данных в компании. В этом блоке на каждый вопрос может быть более одного верного варианта ответа.

10. Для начала Биллу нужно вспомнить что такое "потери данных" в контексте кибербезопасности?

а) Процесс шифрования данных для защиты от утечек
б) Утрата информации в результате повреждения или удаления данных без возможности восстановления
в) Конфиденциальные данные, которые стали доступны посторонним лицам
г) Атака, при которой данные передаются в незащищённом виде

11. Начальник упомянул, что первое, чем стоит заняться Биллу – это рассмотрение атаки MitM. Какие из следующих утверждений о типах атак "Человек посередине" (MITM) являются верными?

а) В MITM-атаке злоумышленник перехватывает и изменяет сообщения между двумя сторонами, при этом обе стороны могут думать, что они общаются напрямую друг с другом
б) Атака MITM невозможна в случае использования SSL/TLS для шифрования данных между клиентом и сервером
в) В MITM-атаке злоумышленник может использовать подмену DNS для перенаправления трафика на фальшивые веб-сайты
г) В MITM-атаке атакующий может только перехватывать данные, но не изменять их

12. Кажется, в ходе проверки журналов был обнаружен “Человек по середине”, при этом даже удалось определить его личность. “ООО Гравити” – это государственное учереждение. Какую ответственность несёт человек, совершивший кибератаку на государственные учреждения?

а) Ответственность только в рамках гражданского права
б) Уголовная ответственность, в том числе за ущерб от утечки данных или разрушение инфраструктуры
в) Только административная ответственность
г) Ответственность только перед владельцем атакуемой сети

Справившегося со своей первой рабочей задачей, Билла перенаправили в серверную на знакомство с местным системным администратором, Фордом. Теперь Биллу предстоит разобраться с вопросами сетевой безопасности компании и возможными уязвимостями сетевой структуры. В этом блоке для каждого вопроса есть один верный вариант ответа.

13. Что такое "DNS-спуффинг" (DNS Spoofing) и как он угрожает безопасности сети?

а) Атака, при которой злоумышленник перенаправляет трафик на поддельный сервер, маскируясь под законный DNS-сервер.
б) Атака, при которой данные на сервере становятся доступными без авторизации.
в) Атака, при которой злоумышленник изменяет данные, передаваемые через DNS-серверы, для их перехвата.
г) Атака, которая скрывает IP-адрес атакующего, маскируя его под другой IP.

14. Что такое "ARP-спуффинг" (ARP Spoofing) и как он может угрожать безопасности сети?

а) Атака, при которой данные, передаваемые по сети, шифруются с помощью слабого алгоритма.
б) Атака, при которой злоумышленник перехватывает все сетевые пакеты, передаваемые между двумя компьютерами.
в) Атака, при которой злоумышленник использует уязвимость в маршрутизаторе для взлома пароля администратора.
г) Атака, при которой злоумышленник подменяет MAC-адрес в ARP-запросах, заставляя устройства сети отправлять данные на его компьютер.

15. Сопоставьте сетевые протоколы с их функциями

1. IPSec	а) Протокол, обеспечивающий защищённое шифрованное соединение для передачи данных по сети, в том числе для веб-сайтов.
2. SSL/TLS	б) Протокол, используемый для передачи данных между устройствами через интернет, но без защиты данных.
3. HTTP	в) Протокол для безопасной передачи данных через IP-сети, часто используется для защиты VPN-соединений.

4. FTP		г) Протокол для передачи файлов между компьютерами по сети, может работать как в защищённом, так и в открытом виде.

Не все так радужно в “ООО Гравити”, и, конечно, на него уже нацелился хакер по имени Гидеон. В этом блоке вам необходимо решить задачи, ответом на вопрос будет решение задачи.

16. Предположим, что злоумышленник пытается угадать пароль, состоящий из 4 символов, где каждый символ — это буква (строчная или заглавная) или цифра. Гидеон ограничен 1000 попыток, какова вероятность что за 1000 попыток Гидеон обнаружит пароль? Дайте ответ в процентах, округлите до тысячных.

17. Алгоритм Base64 – стандарт кодирования двоичных данных при помощи только 64 символов ASCII. Он работает следующим образом. 1. Каждая буква или символ в тексте сначала преобразуется в двоичный код на основе ASCII-кодировки.

2. Полученные двоичные коды объединяются в одну длинную строку.

3. Полученная строка разбивается на группы по 6 бит. 4. Каждая 6-битная группа преобразуется в десятичное число. 5. Каждое число заменяется соответствующим символом из таблицы Base64. Таблица Base64 содержит 64 символа: латинские буквы (A-Z, a-z), цифры (0–9) и два дополнительных символа (+ и /).

Гидеон решил попробовать в качестве пароля попробовать слово Gideon, зашифрованное base64. Зашифруйте слово Gideon.

Letter	ASCII Code	Binary
a	97	01100001
b	98	01100010
c	99	01100011
d	100	01100100
e	101	01100101
f	102	01100110
g	103	01100111
h	104	01101000
i	105	01101001
j	106	01101010
k	107	01101011
l	108	01101100
m	109	01101101
n	110	01101110
o	111	01101111
p	112	01110000
q	113	01110001
r	114	01110010
s	115	01110011
t	116	01110100
u	117	01110101
v	118	01110110
w	119	01110111
x	120	01111000
y	121	01111001
z	122	01111010

Letter	ASCII Code	Binary
A	65	01000001
B	66	01000010
C	67	01000011
D	68	01000100
E	69	01000101
F	70	01000110
G	71	01000111
H	72	01001000
I	73	01001001
J	74	01001010
K	75	01001011
L	76	01001100
M	77	01001101
N	78	01001110
O	79	01001111
P	80	01010000
Q	81	01010001
R	82	01010010
S	83	01010011
T	84	01010100
U	85	01010101
V	86	01010110
W	87	01010111
X	88	01011000
Y	89	01011001
Z	90	01011010

Соответствие символов и их значений в кодировке Base64

Символ	Значение			
	10	2	8	16
A	0	000000	00	00
B	1	000001	01	01
C	2	000010	02	02
D	3	000011	03	03
E	4	000100	04	04
F	5	000101	05	05
G	6	000110	06	06
H	7	000111	07	07
I	8	001000	10	08
J	9	001001	11	09
K	10	001010	12	0A
L	11	001011	13	0B
M	12	001100	14	0C
N	13	001101	15	0D
O	14	001110	16	0E
P	15	001111	17	0F

Символ	Значение			
	10	2	8	16
Q	16	010000	20	10
R	17	010001	21	11
S	18	010010	22	12
T	19	010011	23	13
U	20	010100	24	14
V	21	010101	25	15
W	22	010110	26	16
X	23	010111	27	17
Y	24	011000	30	18
Z	25	011001	31	19
a	26	011010	32	1A
b	27	011011	33	1B
c	28	011100	34	1C
d	29	011101	35	1D
e	30	011110	36	1E
f	31	011111	37	1F

Символ	Значение			
	10	2	8	16
g	32	100000	40	20
h	33	100001	41	21
i	34	100010	42	22
j	35	100011	43	23
k	36	100100	44	24
l	37	100101	45	25
m	38	100110	46	26
n	39	100111	47	27
o	40	101000	50	28
p	41	101001	51	29
q	42	101010	52	2A
r	43	101011	53	2B
s	44	101100	54	2C
t	45	101101	55	2D
u	46	101110	56	2E
v	47	101111	57	2F

Символ	Значение			
	10	2	8	16
w	48	110000	60	30
x	49	110001	61	31
y	50	110010	62	32
z	51	110011	63	33
0	52	110100	64	34
1	53	110101	65	35
2	54	110110	66	36
3	55	110111	67	37
4	56	111000	70	38
5	57	111001	71	39
6	58	111010	72	3A
7	59	111011	73	3B
8	60	111100	74	3C
9	61	111101	75	3D
+	62	111110	76	3E
/	63	111111	77	3F

18. Введя пароль, Гидеон получил в ответ сообщение, так же зашифрованное Base64. Расшифруйте его.
    bGll
19. Поняв, что затея с паролем не удалась – Гидеон решил зашифровать в видеофайле вирус, но для этого ему нужно понять сколько информации он сможет зашифровать в одном файле. У Гидеона есть видеофайл в формате MP4 с разрешением 100x100 пикселей и длительностью 5 минут. Этот файл содержит 30 кадров в секунду (fps), и каждый пиксель имеет максимальный размер 0xFF. Сколько бит информации можно скрыть в 5 минутах видео. Ответ запишите в Мбайтах с округлением до 10ых.
20. Когда Гидеон наконец отправил зараженный файл в компанию, вскоре получил короткий зашифрованный ответ. Расшифруйте, какое сообщение получил Гидеон.
    00010001 00010010 00010000 00000011 00000001 00001101
21. Последней попыткой Гидеона достучаться до сайта компании, вам же нужно выяснить какую информацию он смог получить от команды.

```
root@debian:~# curl -v www.gravity.com
*   Trying 10.0.0.10:80...
* Connected to www.gravity.com (10.0.0.10) port 80 (#0)
> GET / HTTP/1.1
> Host: www.gravity.com
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Server: nginx/1.25.3
< Date: Wed, 27 Nov 2024 23:16:01 GMT
< Content-Type: text/html
< Content-Length: 237
< Last-Modified: Sun, 11 Feb 2024 18:43:28 GMT
< Connection: keep-alive
< ETag: "65c91550-ed"
< Accept-Ranges: bytes
<
<!DOCTYPE html>
<html>
    <head>
        <title>Home Page</title>
    </head>
    <body>
        <h1>Home Page</h1>
        <p>This is a public web page. You may also visit <a href="private/">a private page</a>.</p>
    </body>
</html>
* Connection #0 to host www.gravity.com left intact
```

1. Через какой порт было произведено подключение к сайту?
2. Какой протокол используется для подключения? Почему сейчас не советуется работать с данным протоколом?
3. Что означает термин “keep-alive connection”?
4. Какой метод запроса используется в данном случае?
5. Можно ли этот метод использовать для передачи паролей? Почему?