

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТЕХНОЛОГИИ
РЕГИОНАЛЬНЫЙ ЭТАП
ТЕОРЕТИЧЕСКИЙ ТУР

11 класс

Профиль «Информационная безопасность»

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:

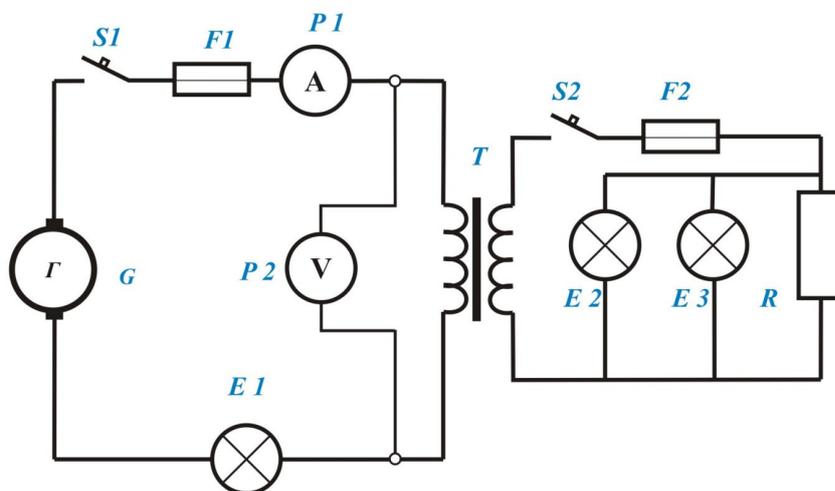
- при оценке тестовых заданий, где необходимо определить один правильный ответ, 0 баллов выставляется за неверный ответ и в случае, если участником отмечены несколько ответов (в том числе правильный), или все ответы;
- при оценке тестовых заданий, где необходимо определить все правильные ответы, 0 баллов выставляется, если участником отмечены неверные ответы, большее количество ответов, чем предусмотрено в задании (в том числе правильные ответы) или все ответы.

Задание теоретического тура считается выполненным, если Вы вовремя сдаете его членам жюри.

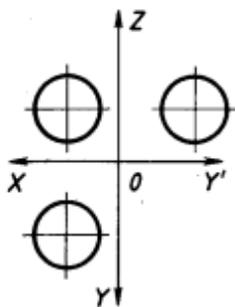
Максимальная оценка – 30 баллов (из них кейс-задание оценивается в 5 баллов).

Общая часть

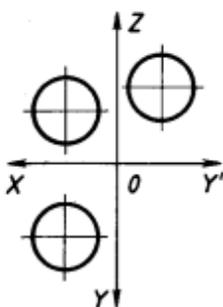
1. Назовите систему, используемую в промышленности, которая позволяет объектам собирать и обмениваться данными в реальном времени, а также анализировать эти данные с помощью компьютерных систем. Она может использоваться для повышения эффективности производства, оптимизации бизнес-процессов и улучшения качества продукции. Его суть заключается в том, что различные устройства и оборудование, используемые на предприятии, могут быть оснащены датчиками и соединены в сеть, что позволяет им собирать разнообразные данные о своей работе. Эти данные передаются в центральные вычислительные системы, где происходит их анализ. Благодаря этому, компании получают возможность контролировать производственные процессы в режиме реального времени, что открывает новые перспективы для повышения эффективности и точности производственной деятельности.
2. В аббревиатуре «UX/UI-дизайн» сокращением каких словосочетаний получили «UX» и «UI»?
3. Впишите в таблицу бланка ответов названия элементов электрической цепи.



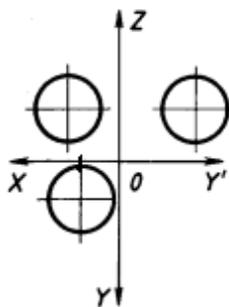
4. На чертежах *а*, *б*, *в* изображено движение шара относительно исходной позиции. В таблице бланка ответов поставьте галочку в ячейке соответствующей оси (соответствующим осям), по которой (по которым) осуществляется перемещение шара на чертежах.



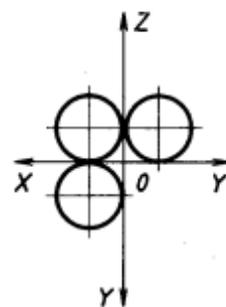
Исходная позиция



а



б



в

5. Организации и ИП, которые отнесены в соответствии с условиями, установленными Федеральным законом от 24.07.2007 № 209-ФЗ (в последней редакции), к малым и средним предприятиям, именуется субъектами малого и среднего предпринимательства. Принято деление таких организаций на малые и средние предприятия. Среди малых предприятий выделяются микропредприятия. Укажите предельные (максимальные) значения среднесписочной численности работников и величины доходов предприятий, заполнив таблицу в бланке ответов.

6. Выберите все виды кибератак, от которых полностью или частично поможет защититься менеджер паролей. Укажите номера выбранных ответов через запятую.

1. Атака методом подбора паролей
2. Атака перебором по словарю паролей
3. Атака с подменой веб-сайта
4. Методы социальной инженерии, в результате которых злоумышленник путём обмана и манипуляций пытается узнать пароли у пользователя

7. Агроном Петя решил взять в аренду гексакоптер для видеосъемки колхозных полей общей площадью 3000 га (1 га = 0,01 км²). В магазине предлагались дроны с разной производительностью и потреблением тока (Таблица 1), а также отдельно аккумуляторы для них (Таблица 2).

Таблица 1. Гексакоптеры

№	Потребление тока, А	Производительность съемки, км ² /ч
А	30	5
Б	50	10
В	70	15
Г	80	20
Д	120	25

Таблица 2. Аккумуляторы

№	Емкость аккумулятора, мАч
1	10000
2	12000
3	15000
4	25000
5	30000

Помогите Пете выбрать такие дрон и аккумулятор наименьшей емкости, чтобы справиться с работой за один световой день 12 часов. Петя возьмет в аренду также зарядное устройство типа CC-CV Charger, так что время полной зарядки любого аккумулятора будет равным 1 ч. В начале работы аккумулятор полностью заряжен. Временем на полет к месту съемки и возврат к зарядному устройству пренебречь. Ответ дайте в формате «буква с цифрой», например: Е6.

8. Какая профессия соответствует следующему описанию?

«Отвечает за проверку и оценку работы роботов. Выявляет и устраняет ошибки, а также обеспечивает соответствие роботов установленным стандартам и требованиям».

- а – инженер по системам управления
- б – программист робототехники
- в – инженер по тестированию и качеству
- г – сервисный инженер-робототехник

Специальная часть

9. При подготовке заданий к региональному этапу ВсОШ подготовленные материалы подверглись воздействию вредоносного программного обеспечения. Условие этого номера было искажено. Определите задание и выполните инструкцию, описанную в нем.

**вКРfотИвеПтТтзаОпГиРАшФРиИтЯгтЭТеОкКtРоБблиwwwчеЫс
тИЕвоПРwmјесЛяцqАевЙвсГгойГдуіИциВиифрЕvawmГи**

Шифр, известный как шифр Плейфера, заключается в замене пар символов, стоящих один за другим (биграмм), на пары символов того же алфавита. Замена происходит по следующему принципу: символы алфавита вносятся в прямоугольную таблицу в произвольном порядке, например, так:

Ц	Ь	Х	Ш	Э	Й
И	В	Ъ	Щ	З	Ю
О	Ы	Г	У	Б	К
Ч	А	Ф	Ж	Я	.
_	М	Р	Н	Т	Е
П	Ё	Л	С	Д	,

Открытый текст разбивается на биграммы. Каждая из них зашифровывается по следующему набору правил:

- Если символы биграммы находятся в одной строке, то каждый из них заменяется на его соседа справа. Для буквы в крайнем правом столбце соседом справа будет считаться буква той же строки из крайнего левого

столбца. Например, «ЪЗ» зашифровывается парой «ЩЮ» (для каждой буквы сосед берется независимо), «МЕ» – «Р_».

- Совпадающие буквы считаются стоящими в одной строке (например, «ЛЛ» – «СС»).
- Если символы биграммы находятся в одном столбце, то каждый из них заменяется на его соседа сверху. Для буквы в самой верхней строке соседом сверху будет считаться буква того же столбца из самой нижней строки. Например, «МВ» – «АЬ», «ПЦ» – «_П».
- Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника. Например, «ТГ» – «РБ», «ТК» – «ЕБ».

10. С помощью шифра Плейфера с ключом из условия зашифруйте сообщение:

КОМПЬЮТЕРНЫЙВИРУСБЫЛОБНАРУЖЕН.

11. Расшифруйте сообщение «Л_Б_ЬЮГП» с помощью шифра Плейфера, используя тот же ключ.

Известно, что для шифрования новой фразы использовался квадрат, заполненный следующим образом: начиная с первой верхней строки, двигаясь слева направо, были вписаны последовательно символы алфавита, из которого состоит сообщение, полученное в задании № 10, а затем были вписаны в алфавитном порядке символы русского алфавита, которые не встретились в полученном ранее сообщении. В последние три ячейки таблицы были вписаны последовательно символы «_», «,» и «.».

Пример: если бы в задании № 10 было получено слово ПРОСТОТА, то в таблицу сначала бы были вписаны последовательно символы П, Р, О, С, Т, А, а затем были бы вписаны символы Б, В, Г, Д, Е, Ё и так далее до последних трёх ячеек, в которые были бы последовательно вписаны символы «_», «,» и «.».

Также известно, что при шифровании были изменены некоторые правила из №10:

- Если символы биграмм находятся в одной строке или в одном столбце, то шифрование теперь осуществлялось в противоположном направлении (берутся соседи слева, а не справа, снизу, а не сверху).
- Если символы биграмм исходного текста находятся в разных столбцах и разных строках, то в процессе шифрования они заменялись на символы, полученные параллельным переносом исходных символов. Для определения символов замены требуется мысленно расположить символы открытого текста так, чтобы соединяющий их отрезок являлся одной из сторон параллелограмма. Символы замены должны находиться в тех же столбцах, что и соответствующие им символы открытого текста, и быть на одном и том же расстоянии от соответствующих символов открытого текста (например, если был выполнен параллельный перенос на 1 ячейку вверх, то символы замены будут находиться на 1 ячейку выше символов открытого текста). Тогда отрезок, соединяющий символы замены, будет представлять собой вторую сторону параллелограмма. Параллельный перенос по величине и направлению остаётся постоянным для каждой из биграмм.

12. Расшифруйте сообщение «ЁЦЖЦСЗПЛНЖРКЦЫ» с помощью шифра Плейфера, пользуясь новыми правилами шифрования. Известно, что исходное сообщение имеет отношение к одному из методов атаки.

При разработке новой олимпиады по математике организаторы решили выделить три отдельных направления: знание математических законов, умение быстро осуществлять сложные вычисления и способность применять известные приемы к нестандартным ситуациям. Соревнования по каждому из направлений проводятся в одной системе, но на разных площадках. Для исключения утечек заданий было решено применить систему разграничения доступа, на основании которой предоставить каждому из действующих лиц свой набор прав. В реализации олимпиады принимают участие разработчики заданий (отдельно для каждого из направлений), эксперты, перекрестно проверяющие задания всех направлений, а также ответственные лица (оргкомитет) площадок проведения, подготавливающие комплекты заданий для участников соответствующего направления.

Для реализации прав доступа была избрана дискреционная модель, при этом матрица прав доступа для перечисленных субъектов и объектов заполнена

следующим образом (здесь наличие права доступа только на чтение отмечено как «10», на чтение и запись – «11», отсутствие прав – «00»):

		Материалы направления №1	Материалы направления №2	Материалы направления №3
1	Разработчики материалов направления №1	11	00	00
2	Разработчики материалов направления №2	00	11	10
3	Разработчики материалов направления №3	00	00	11
4	Эксперты	11	11	11
5	Оргкомитет направления №1	11	10	10
6	Оргкомитет направления №2	00	11	00
7	Оргкомитет направления №3	10	11	10

13. Установите категории пользователей, наборы прав которых нарушают принципы разграничения доступа.

14. Установите, возможны ли несанкционированный доступ и несанкционированная модификация материалов всех направлений при компрометации (взломе) учетной записи ровно одного из членов оргкомитета какого-нибудь (на выбор нарушителя) из направлений. В ответе укажите:

«00», если обе угрозы реализовать таким образом невозможно,
«10», если можно реализовать только несанкционированный доступ,
«01», если можно реализовать только несанкционированную модификацию
«11», если можно реализовать обе угрозы.

15. Определите, учетные записи разработчиков из какого числа направлений (по выбору нарушителей) достаточно скомпрометировать для успешного внесения несанкционированных изменений в материалы олимпиады при условии, что все нарушения принципов разграничения доступа, возможно присутствующие в системе, будут устранены. Укажите минимальное необходимое число скомпрометированных учетных записей для успешной

реализации угрозы или «0», если компрометация учетных записей разработчиков не позволяет ее реализовать.

Отправителю требуется передать сообщение длиной 11 бит, обеспечив отсутствие в нем ошибок. Для этого сообщение кодируется кодовым словом (двоичной последовательностью) $x_1x_2x_3x_4 \dots x_{11}$. Далее к нему добавляются символы $x_{12}, x_{13}, x_{14}, x_{15}$, определяемые следующими равенствами по модулю 2:

$$x_{12} = x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus x_9 \oplus x_{10} \oplus x_{11}$$

$$x_{13} = x_2 \oplus x_3 \oplus x_4 \oplus x_8 \oplus x_9 \oplus x_{10} \oplus x_{11}$$

$$x_{14} = x_1 \oplus x_3 \oplus x_4 \oplus x_6 \oplus x_7 \oplus x_{10} \oplus x_{11}$$

$$x_{15} = x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_7 \oplus x_9 \oplus x_{11}$$

16. Требуется выяснить, допущена ли при передаче сообщения $x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}x_{11}x_{12}x_{13}x_{14}x_{15}$ единичная ошибка, и если да, то в каком бите. Известно, что если ошибка все же произошла, то ее положение можно определить с помощью значений добавленных символов $x_{12}, x_{13}, x_{14}, x_{15}$.

В ответ запишите исправленное (если требуется) сообщение **100101100101110**.

17. В ответ укажите символ, если первые 7 битов слева результата выполнения предыдущего задания - двоичная запись кода символа в таблице ASCII.

32	SP	48	0	64	@	80	P	96	`	112	p
33	!	49	1	65	A	81	Q	97	a	113	q
34	"	50	2	66	B	82	R	98	b	114	r
35	#	51	3	67	C	83	S	99	c	115	s
36	\$	52	4	68	D	84	T	100	d	116	t
37	%	53	5	69	E	85	U	101	e	117	u
38	&	54	6	70	F	86	V	102	f	118	v

39	'	55	7	71	G	87	W	103	g	119	w
40	(56	8	72	H	88	X	104	h	120	x
41)	57	9	73	I	89	Y	105	i	121	y
42	*	58	:	74	J	90	Z	106	j	122	z
43	+	59	;	75	K	91	[107	k	123	{
44	,	60	<	76	L	92	\	108	l	124	
45	-	61	=	77	M	93]	109	m	125	}
46	.	62	>	78	N	94	^	110	n	126	~
47	/	63	?	79	O	95	_	111	o	127	DE L

Антон только что узнал о шифре замены. Чтобы попрактиковаться, он решил зашифровать открытый текст с помощью математической функции $E(x)$, где x - номер шифруемой буквы открытого текста в английском алфавите, пронумерованном с нуля. Значения функции в каждой точке области определения указывают на номер буквы, на которую происходит замена.

18. Помогите Антону выбрать все подходящие функции, которые гарантируют однозначный процесс шифрования и расшифрования.

- 1) $E(x) = 2x + 9 \pmod{26}$
- 2) $E(x) = 13 \sin(x) + 10 \cos(x) + 15 \pmod{32}$
- 3) $E(x) = 7x + 13 \pmod{26}$
- 4) $E(x) = x^2 \pmod{26}$

19. Зашифруйте слово **COMPETITION** с помощью функций, выбранных в предыдущем задании. В ответ запишите получившиеся шифртексты через запятую.

Известно, что для шифрования стихотворения Агнии Барто «В школу» использовалась некая функция $E(x)$, где x - номер шифруемой буквы открытого текста в русском алфавите, пронумерованном с нуля. Значения функции в

каждой точке области определения указывают на номер буквы, на которую происходит замена.

Открытый текст	Шифртекст
Почему сегодня Петя Просыпался десять раз? Потому что он сегодня Поступает в первый класс.	Пжхпхт бпюжжюы Ппйы Пшжбшпдмбы жпбыйб шдй? Пжйжхт хйж жю бпюжжюы Пжбйтпдпй х ппшхшы дмдбб.
Он теперь не просто мальчик, А теперь он новичок. У него на новой куртке Отложной воротничок.	Жю йпппшб юп пшжбйж хдмбхтд, Д йпппшб жю южхтхжд. Т юпюж юд южхжы дтшйдп Жймжбюжы хжшжйютхжд.

20. Укажите функцию, с помощью которой было зашифровано стихотворение Агнии Барто “В школу”.

21. Для анализа сетевых пакетов используются программы, известные как сетевые анализаторы. Перед Вами скриншот части окна одной из таких программ. Определите, какой IP-адрес у отправителя пакета.

```

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 70
  Identification: 0x3eb1 (16049)
> Flags: 0x00
  Fragment offset: 0
  Time to live: 128
  Protocol: UDP (17)
> Header checksum: 0x23a5 [validation disabled]
  Source: 10.33.32.81
  Destination: 172.19.1.204

```

```

0000  00 15 62 b0 8c f6 80 56 f2 2d 91 85 08 00 45 00  ..b....V .-....E.
0010  00 46 3e b1 00 00 80 11 23 a5 0a 21 20 51 ac 13  .F>....#!Q..
0020  01 cc c0 00 00 a1 00 32 be e5 30 28 02 01 00 04  .....2 ..0(...
0030  06 70 75 62 6c 69 63 a1 1b 02 02 01 3f 02 01 00  .public. ....?...
0040  02 01 00 30 ef 30 0d 06 09 2b 06 01 04 01 95 0b  ...0.0.. +.....
0050  01 02 05 00  ....

```

22. На следующем скриншоте из той же программы выделены заголовок и данные ICMP-протокола. Укажите, чему равна контрольная сумма в десятичной системе счисления.

```

> Frame 1149: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: HonHaiPr_2d:91:85 (80:56:f2:2d:91:85), Dst: RealtekU_71:75:11 (52:54:00:71:75:11)
> Internet Protocol Version 4, Src: 172.19.4.82, Dst: 8.8.8.8
> Internet Control Message Protocol

0000  52 54 00 71 75 11 80 56 f2 2d 91 85 08 00 45 00  RT.qu..V .-....E.
0010  00 3c 75 06 00 00 80 01 05 46 ac 13 04 52 08 08  .<U.....F...R..
0020  08 08 08 00 4d 33 00 01 00 28 61 62 63 64 65 66  ...MJ...{abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklm opqrstuv
0040  77 61 62 63 64 65 66 67 68 69  wabcedfg hi

```

23. Для описания компьютерных атак в форме, удобной для обмена информацией между специалистами в области информационной безопасности, могут использоваться различные подходы. Один из них заключается в представлении атаки в виде последовательности действий нарушителя, разделенной на несколько этапов, на каждом из которых нарушитель стремится достичь некоторой промежуточной цели. Такие шаги обычно называются тактиками. Конкретные действия нарушителя по реализации тактики называются техниками.

Перед Вами описание компьютерной атаки, а также ряд тактик, которыми обычно пользуются злоумышленники в своих атаках на корпоративную инфраструктуру, и соответствующих им техник.

Нанятый конкурирующей организацией нарушитель начал атаку, отправив зараженное вложение через электронную почту сотруднику компании. Сотрудник открыл файл, в результате чего на его рабочем компьютере был загружен вредоносный скрипт. Этот скрипт установил соединение с удаленным сервером злоумышленника, предоставляя обратный доступ к системе. Получив доступ, злоумышленник нашел учетные данные, сохраненные в текстовом файле. Эти учетные данные позволили ему подключиться к другому серверу внутри корпоративной сети. После подключения злоумышленник поместил финансовую отчетность компании и другую конфиденциальную информацию в зашифрованный архив. Архив был отправлен на сервер злоумышленника, используя легитимный протокол передачи файлов и облачное хранилище данных в качестве промежуточного узла.

Соотнесите действия нарушителя из приведенного описания с подходящими тактиками и соответствующими им техниками из предложенных – составьте тройки вида «тактика – техника – действие нарушителя», сформировав сценарий описанной атаки.

Тактики:

- Подготовка ресурсов
- Первоначальный доступ
- Выполнение
- Закрепление
- Повышение привилегий
- Получение учетных данных
- Организация управления
- Сбор данных
- Перемещение внутри периметра
- Сбор информации
- Эксфильтрация данных

Техники

- Архивация собранных данных
- Вредоносный файл
- Данные из локальной системы
- Изучение сетевых служб
- Манипуляции с учетной записью
- ПО для удаленного доступа
- Службы удаленного доступа
- Учетные данные в файлах
- Целевой фишинг с вложением
- Эксфильтрация через веб-службу