ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ

Разбор заданий школьного этапа всероссийской олимпиады школьников по технологии (информационная безопасность) 10-11 класс

2024/2025 учебного года в Свердловской области

Разработчик –
Алексеевский Петр Иванович,
ст. преп. кафедры ИИТиМОИ
УрГПУ

Виды заданий

- Общие теоретические вопросы:
  - с одним правильным вариантом ответа;
  - с несколькими вариантами ответа (обычно с двумя).
- Вычислительные задачи.
- Задания-головоломки на тему криптографии.

Классификация вредоносного ПО

Вид ПО	Определяющая характеристика
Вирус	Распространение путём встраивания собственного программного кода в исполняемые модули (как на устройствах хранения, так и непосредственно в ОЗУ).
Червь	Распространение с использованием уязвимостей в программном обеспечении (преимущественно сетевом - «сетевые черви»).
Троян	Распространение с использованием методов социальной инженерии (т. е. в конечном итоге виноват пользователь).
Malware	«Malfunctioning software», условно-вредоносное ПО, нарушающее работу информационной среды из-за допущенных при разработке ошибок.

Таким образом, ответы на вопрос 6 следующие:
Вариант I: Д (социальная инженерия)
Вариант II: Г (распространение по сети)

Основные компоненты информационной безопасности

- Конфиденциальность — свойство информации, предполагающее невозможность доступа к ней третьих лиц.
- Целостность — свойство информации, предполагающее неизменность её с момента создания или модификации доверенным субъектом.
- Доступность — свойство информации, предполагающее наличие возможности доступа к информации субъектами, имеющими на это право, в любой разрешённый момент времени.

Таким образом, ответы на вопросы 7-8 и 10-12:
Вариант I: 7 — Б, 8 — Б, 10 — А,Б, 11 — Б, 12 — В
Вариант II: 7 — А, 8 — Б, 10 — Б,Г, 11 — А, 12 — Б

Правовые основы информационной безопасности

- Законодательство РФ предусматривает более 80 видов тайн.
- Существует информация, которая не может составлять никакую тайну, и обязана находиться в свободном доступе.
- С каждым видом тайны связан по крайней мере один федеральный закон (обычно больше).

Правовые основы информационной безопасности

- Информацию о государственных ведомствах и их деятельности можно узнать на сайтах этих ведомств (см. раздел «документы» или аналогичный):
  - Федеральная служба по техническому и экспортному контролю
    - https://fstec.ru/
  - Министерство обороны
    - https://mil.ru/
  - Министерство промышленности и торговли
    - https://minpromtorg.gov.ru/
  - Министерство цифрового развития
    - https://digital.gov.ru/ru/
  - Федеральная служба безопасности
    - http://www.fsb.ru/

Правовые основы информационной безопасности

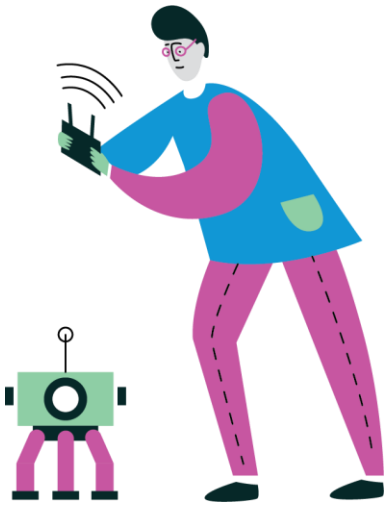
- Банк данных угроз безопасности — https://bdu.fstec.ru/, располагается на сайте ФСТЭК.
- Реестр радиоэлектронной продукции находится в Государственной информационной системе промышленности — https://gisp.gov.ru/, являющейся частью ресурсов Минпромторга.
- Реестр отечественного ПО находится на сайте Минцифры — https://reestr.digital.gov.ru/.
- Вариант I: 9 — Г.
- Вариант II: 9 — А.

Программные средства защиты информации

- На серверах в Интернете наиболее распространены UNIX-подобные операционные системы, в частности — GNU/Linux. (Вариант I, 14 - В)
- Oracle VirtualBox является решением для «настольной» виртуализации. Несмотря на возможность использования данной платформы на серверах, такой режим работы не имеет полноценной технической поддержки, стабильность работы платформы в целом не гарантируется, а интеграция с распространёнными средствами администрирования зачастую отсутствует (несмотря на наличие соответствующего API). (Вариант II, 14 — А)

Технические средства обеспечения информационной безопасности

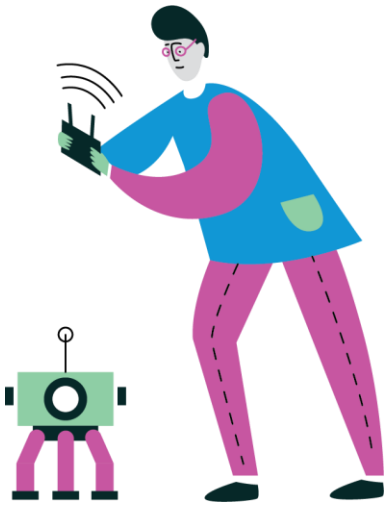
- Криптографические токены, смарт-карты и другие похожие устройства — представляют собой доверенное хранилище реквизитов (как криптографических ключей, так и алгоритмов, выполняющихся на самой смарт-карте). Токены (выглядят как USB Flash-накопители, хотя таковыми не являются) обычно представляют собой смарт-карту и устройство для работы с ней, объединённые в единую конструкцию.



Вариант I: 14 — В
Вариант II: 24 — Г

Технические средства обеспечения информационной безопасности

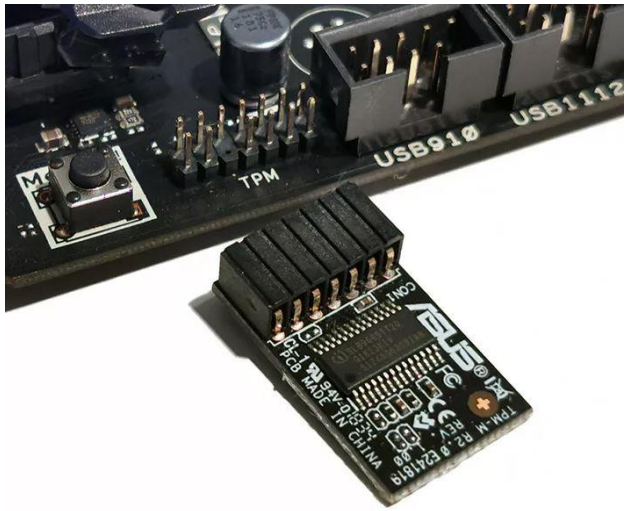
- OTP-генераторы — устройства для генерации одноразовых паролей с помощью специальных алгоритмов. За исключением кнопки включения и дисплея, обычно не имеют никаких средств взаимодействия с внешним миром. Для вычисления ключа используют встроенные часы, синхронизированные с сервером.

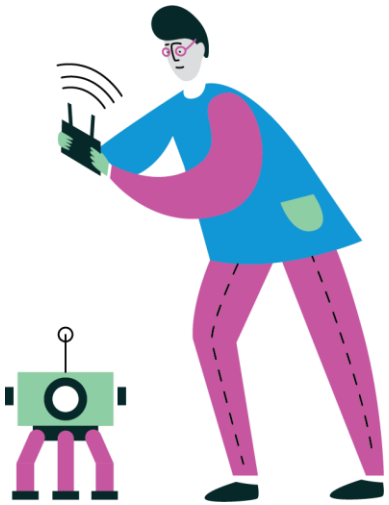


Вариант I: 14 - Г

Технические средства обеспечения информационной безопасности

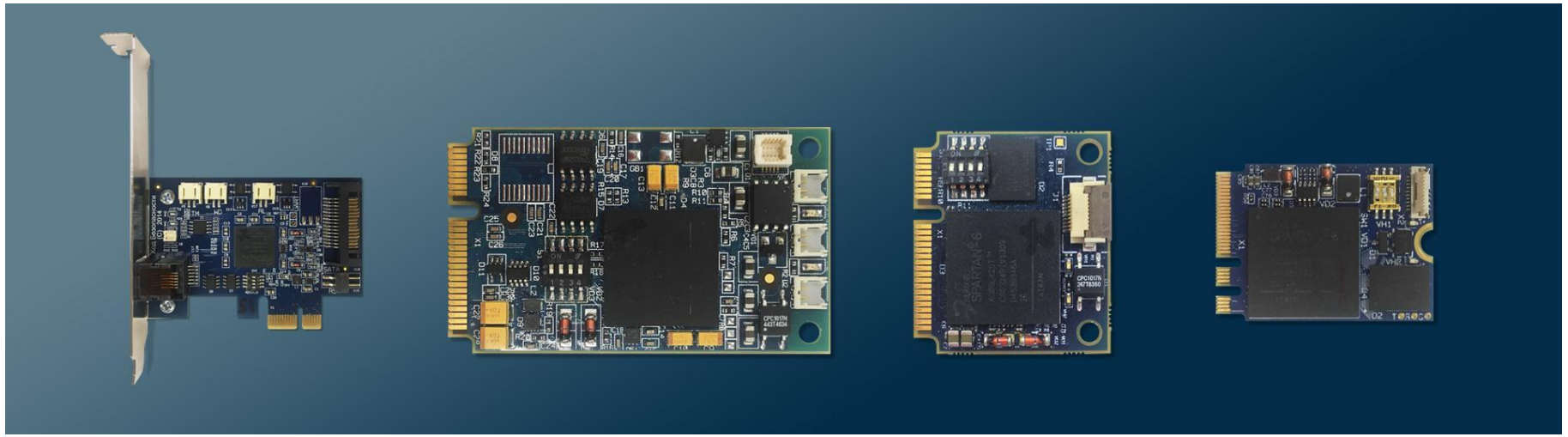
- TPM-модуль — специализированное устройство, реализующее функции доверенного хранилища ключей, криптопроцессора и датчика случайных чисел. (Вариант I, 13 — В)
- Если какое-либо криптографическое ПО использует этот модуль, то его извлечение приводит к невозможности работы этого ПО, в том числе, к невозможности загрузки ОС, если содержимое жёсткого диска зашифровано хранящимся в модуле ключом.

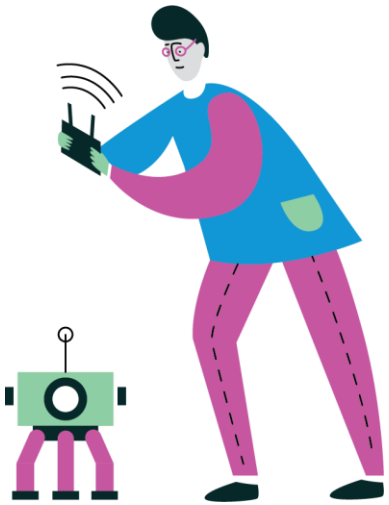




Технические средства обеспечения информационной безопасности

- Модуль доверенной загрузки — специальное устройство, делающее невозможным использование компьютера в случае изменения его конфигурации или попытки несанкционированного доступа к данным. В общем случае осуществляет контроль целостности конфигурации компьютера и обеспечивает запуск только доверенной операционной системы. Некоторые МДЗ содержат также контроллер жёсткого диска с прозрачным шифрованием всех записываемых данных.
(Вариант I: 24 — Б. Вариант II: 13 — Г)

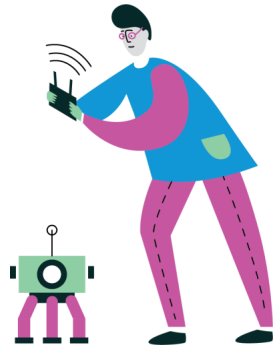




ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ
ТЕХНОЛОГИЯ
ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ

Технические средства обеспечения информационной безопасности

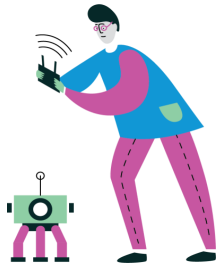


- RAID (Redundant Array of Independent Disks, избыточный массив самостоятельных дисков) — одна из технологий повышения надёжности (отказоустойчивости) и/или производительности подсистемы хранения данных.
- Модель RAID имеет несколько уровней, среди которых наиболее распространены представленные в соответствующем задании 0, 1, 5, 6, 1+0, 5+0.
- Уровень 0 предназначен для повышения производительности, обычно в ущерб надёжности
- Уровень 1 — полное дублирование данных на нескольких дисках, и этот вариант мог бы быть правильным ответом на вопрос, если бы присутствовал в списке как самостоятельный.
- Уровни 5 и 6 добавляют избыточность с использованием различных алгоритмов, и допускают выход из строя соответственно любого одного или двух дисков.
- «Гибридные» уровни 1+0 и 5+0 позволяют повысить производительность, в какой-то мере сохраняя надёжность (но не повышая её).
- Правильным ответом на задание 18 варианта II является Д. RAID 6 — единственный уровень из предлагаемых, допускающий выход из строя одновременно двух любых дисков.

ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ
ТЕХНОЛОГИЯ
ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ

Технические средства обеспечения информационной безопасности



- Резервное копирование — важный элемент обеспечения информационной безопасности. Оно может осуществляться на различные съёмные носители информации. При большом объёме информации, подлежащей резервному копированию, важным параметром становится стоимость хранения информации на таких носителях.
- Самый простой способ оценить стоимость хранения информации — разделить стоимость носителя на его объём. Впрочем, в реальности формула расчёта несколько сложнее, поскольку следует также учитывать срок службы носителей, а также затраты электроэнергии и [однократные] затраты на устройство для работы с этими носителями.
- Пример: жёсткий диск объёмом 4ТБ стоит 11800р, а диск объёмом 6ТБ — 14400р. Таким образом, стоимость хранения одного ТБ информации составляет 2950р и 2400р соответственно. Если требуемый объём хранилища — 24ТБ, то по данному показателю выгоднее использовать не 6 дешёвых дисков объёмом 4ТБ (70800р), а 4 более дорогих диска по 6ТБ (57600р).
- Стоимость ленточного картриджа LTO-8 объёмом 12ТБ (30ТБ со сжатием) на момент написания данного текста составляет около 9700р, таким образом, стоимость хранения 1ТБ будет составлять 808р (323р со сжатием).
- На данный момент при больших объёмах резервного копирования магнитная лента является (с очень большим разрывом) наиболее дешёвым носителем информации. (Вариант I: 1

Программные средства обеспечения информационной безопасности

- Base64-кодирование — один из способов кодирования двоичных данных, позволяющий передавать их без повреждений через каналы связи, рассчитанные на передачу текстовой информации. Наиболее распространённый пример — электронная почта. Протоколы SMTP, IMAP, POP3 ориентированы на работу с текстовой информацией, поэтому все двоичные данные (например, файлы во вложениях) должны быть закодированы в виде текста (кстати, это главная причина увеличения размера отправляемого электронного письма на треть по сравнению с отправляемым файлом).

- Кодирование заключается в разбиении потока двоичных данных на блоки по 6 бит (2^6=64, отсюда название) и замене полученных значений символами алфавита. Для электронной почты используется способ кодирования, описанный в RFC 4648, параграф 4. Этот способ предлагает следующий алфавит (а также символ «=» для выравнивания):

00_{16}	A	08_{16}	I	10_{16}	Q	18_{16}	Y	20_{16}	g	28_{16}	o	30_{16}	w	38_{16}	4
01_{16}	B	09_{16}	J	11_{16}	R	19_{16}	Z	21_{16}	h	29_{16}	p	31_{16}	x	39_{16}	5
02_{16}	C	$0A_{16}$	K	12_{16}	S	$1A_{16}$	a	22_{16}	i	$2A_{16}$	q	32_{16}	y	$3A_{16}$	6
03_{16}	D	$0B_{16}$	L	13_{16}	T	$1B_{16}$	b	23_{16}	j	$2B_{16}$	r	33_{16}	z	$3B_{16}$	7
04_{16}	E	$0C_{16}$	M	14_{16}	U	$1C_{16}$	c	24_{16}	k	$2C_{16}$	s	34_{16}	0	$3C_{16}$	8
05_{16}	F	$0D_{16}$	N	15_{16}	V	$1D_{16}$	d	25_{16}	l	$2D_{16}$	t	35_{16}	1	$3D_{16}$	9
06_{16}	G	$0E_{16}$	O	16_{16}	W	$1E_{16}$	e	26_{16}	m	$2E_{16}$	u	36_{16}	2	$3E_{16}$	+
07_{16}	H	$0F_{16}$	P	17_{16}	X	$1F_{16}$	f	27_{16}	n	$2F_{16}$	v	37_{16}	3	$3F_{16}$	/

Программные средства обеспечения информационной безопасности

- Решение заданий на кодирование: (вопрос 21)

<table>
<tr><td colspan="8">R</td><td colspan="8">A</td><td colspan="8">D</td><td colspan="8">I</td><td colspan="8">O</td><td colspan="8"></td></tr>
<tr><td colspan="8">82_{10}</td><td colspan="8">65_{10}</td><td colspan="8">68_{10}</td><td colspan="8">73_{10}</td><td colspan="8">79_{10}</td><td colspan="8"></td></tr>
<tr><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="6">14_{16}</td><td colspan="6">24_{16}</td><td colspan="6">05_{16}</td><td colspan="6">04_{16}</td><td colspan="6">12_{16}</td><td colspan="6">14_{16}</td><td colspan="6">$3C_{16}$</td><td colspan="6"></td></tr>
<tr><td colspan="6">U</td><td colspan="6">k</td><td colspan="6">F</td><td colspan="6">E</td><td colspan="6">S</td><td colspan="6">U</td><td colspan="6">8</td><td colspan="6">=</td></tr>
</table>

<table>
<tr><td colspan="8">W</td><td colspan="8">A</td><td colspan="8">V</td><td colspan="8">E</td><td colspan="8"></td><td colspan="8"></td></tr>
<tr><td colspan="8">87_{10}</td><td colspan="8">65_{10}</td><td colspan="8">86_{10}</td><td colspan="8">69_{10}</td><td colspan="8"></td><td colspan="8"></td></tr>
<tr><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="6">15_{16}</td><td colspan="6">34_{16}</td><td colspan="6">05_{16}</td><td colspan="6">16_{16}</td><td colspan="6">11_{16}</td><td colspan="6">10_{16}</td><td colspan="6"></td><td colspan="6"></td></tr>
<tr><td colspan="6">V</td><td colspan="6">0</td><td colspan="6">F</td><td colspan="6">W</td><td colspan="6">R</td><td colspan="6">Q</td><td colspan="6">=</td><td colspan="6">=</td></tr>
</table>

Программные средства обеспечения информационной безопасности

- Решение заданий на декодирование: (вопрос 20)

- Буква А имеет код 65 (64+**1**, первая буква), т.о. для получения порядкового номера буквы (считая от 1) следует из кода вычесть 64

T	1	J	B	T	k	d	F
13_{16}	35_{16}	09_{16}	01_{16}	13_{16}	24_{16}	$1D_{16}$	05_{16}
0 1 0 0 1 1 1 1	0 1 0 1	0 0 1 0	0 0 0 0 0 0 0 1	0 1 0 0 1 1 1 0	0 1 0 0	0 1 1 1	0 1 0 0 0 1 0 1
79_{10}=64+15	82_{10}=64+18	65_{10}=64+1	78_{10}=64+14	71_{10}=64+7	70_{10}=64+5		
O	R	A	N	G	E		

Q	k	F	O	Q	U	5	B
10_{16}	24_{16}	05_{16}	$0E_{16}$	10_{16}	14_{16}	39_{16}	01_{16}
0 1 0 0 0 0 1 0	0 1 0 0	0 0 0 0 1 0 1 0	0 1 1 1 0	0 1 0 0 0 0 0 1	0 1 0 1 0 0	1 1 1 0	0 1 0 0 0 0 0 1
66_{10}=64+2	65_{10}=64+1	78_{10}=64+14	65_{10}=64+1	78_{10}=64+14	65_{10}=64+1		
B	A	N	A	N	A		

Криптография

- Задачи на расшифрование слов, зашифрованных путём сдвига алфавита на некоторое смещение.

- Величина сдвига выбрана достаточно небольшой
- Важно заметить, что зашифровано было **слово**, а значит, в нём не может быть сочетаний букв, которые не встречаются в словах.
- Гарантированно неправильную величину сдвига алфавита можно определить по нескольким буквам, нет необходимости перебирать все варианты.
- Например, зашифрованное сообщение - «ИМОАГР». Попробуем сдвинуть первые две буквы по алфавиту на 1, 2 и 3 позиции в обе стороны:
  ЁЙ ← ЖК ← ЗЛ ← **ИМ** → ЙН → КО → ЛР (жирным шрифтом показан оригинал)
  Из полученных шести вариантов только два могли бы встретиться в начале слова. Добавим ещё одну букву:
  ЗЛН…, КОР… — видно, что первый вариант точно неправильный. Продолжая работать со вторым вариантом, получаем ответ на задание — слово «КОРВЕТ». Зашифровано было путём сдвига алфавита на две позиции назад. Таким образом,
- ЪОЙЕКВУ → ЭСМИНЕЦ (3 позиции назад), НУЗМФЗУ → КРЕЙСЕР (3 позиции вперёд). (Вариант I и II, вопрос 15)

Криптография

- Задачи на расшифрование слов, зашифрованных путём замены алфавита

- Алфавит получен перемешиванием букв в случайном порядке. Этот новый алфавит и является ключом шифрования.
- Для расшифрования сообщения достаточно выполнить обратную замену.

Например, зашифрованное сообщение - «БШЮДБАЪЧЫ ЩЬЫР», таблица замен:

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

Заменяя каждую букву по таблице (находим букву во второй строке, заменяем на букву из первой строки той же колонки), т. е. Б→Т, Ш→Е, Ю→К и т. д., получаем ответ на задание - «ТЕКСТОВЫЙ ФАЙЛ».

Вариант I, 16 — «СЛУЧАЙНОЕ ЧИСЛО»
Вариант II, 16 — «ВВОД ПАРАМЕТРОВ»

ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ


Благодарю за внимание!