

ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

2025–2026 уч. г.

10–11 КЛАССЫ

Максимальный балл за работу – 100.

Общая часть

1. В результате выполнения приведенного алгоритма исполнитель перешел в клетку С4. Укажите координаты исходной клетки.

	А	В	С	Д	Е
1					
2					
3					
4			И		
5					
6					
7					

Если клетка не закрашена

то влево

вниз;

вправо;

вправо;

вниз;

влево;

иначе вниз;

вправо;

вверх;

вправо;

вниз;

вниз;

конец ветвления.

2. Существует ли треугольник (да/нет), длины сторон которого, выражаются числами 12_8 , 11_{16} и 11011_2 ? Свой ответ обоснуйте.
3. Какое минимальное количество бит нужно, чтобы закодировать 500 различных сообщений

4. В компьютерной сети используются IP-адреса из диапазона 192.168.1.0 - 192.168.1.255. Сколько устройств может быть подключено к этой сети?
5. В массиве чисел [1, 5, 3, 8, 2, 9, 4, 7, 6] найти минимальное и максимальное числа. Определите оптимальное количество сравнений, которое потребуется, чтобы наверняка найти и минимальное, и максимальное числа.

Специальная часть

6. В школе используются пароли для доступа к электронному дневнику. Для повышения безопасности в паролях запрещено использовать только буквы или только цифры. Пароль должен содержать как минимум одну букву (латинскую, заглавную или строчную), так и минимум одну цифру. Какой пароль (или пароли):
 а) «School2025»
 б) «school25»
 в) «12345678»
7. В магазине имеются сейфы с замками двух типов. Первый открывается, если каждый из шести его кодовых дисков установить в нужное положение. Каждый диск имеет 100 положений. Второй тип сейфового замка содержит 80 переключателей по два положения у каждого. Сейф открывается только при установке каждого переключателя в нужное положение. Какой сейф надежнее?

8. Разведчик передал в штаб радиogramму: $_ \cdot \cdot _ _ _ \cdot _ _ \cdot _ _ \cdot _ \cdot \cdot$
 В этой радиogramме содержится последовательность букв, в которой встречаются только буквы А, Б, В, Г, Д. Каждая буква закодирована с помощью азбуки Морзе. Разделителей между кодами букв нет.

Запишите в ответе переданную последовательность букв.

Нужный фрагмент азбуки Морзе приведен ниже:

А	Б	В	Г	Д
$\cdot _ _$	$_ _ _ \cdot$	$\cdot$	$_ \cdot$	$_ \cdot _ _$

9. Для зашифрования осмысленного слова его буквы заменили числами $x_1, x_2, \dots, x_n$ по таблице.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Затем выбирали четные натуральные числа p и q и для каждого числа x_i из соотношений $x_i = y_i + pz_i$, $z_i = y_i + qx_i$ нашли целые числа y_i и z_i . Потом по формулам $c_i = r_{32}(z_i)$, $i = 1, \dots, n$ получили числа $c_1, \dots, c_n$ (где $r_{32}(a)$ – остаток от деления числа a на 32), которые вновь заменили буквами согласно таблице. В результате

получили: ЖЯЮЦКР. Найдите исходное слово, если известно, что оно начинается на букву В.

10. Про составленный из цифр 9-значный пароль ($a_1, a_2, \dots, a_9$) известно следующее:

- 1) сумма первых 5 цифр $a_1 + \dots + a_5$ делится на 5,
- 2) сумма всех цифр пароля $a_1 + \dots + a_9$ делится на 10.

Сколько таких паролей?

11. Злоумышленник собирается скрыть текстовое сообщение в видеофайле без звука длительностью 3 минуты. Видео имеет разрешение 100x80 пикселей и частоту 24 кадра в секунду. В каждом кадре максимальное значение интенсивности каждого из цветов составляет 0xFF. Злоумышленник будет использовать метод LSB для скрытия информации в каждом пикселе каждого RGB-кадра. Сколько символов он сможет скрыть в этом видеофайле, заменяя по одному значащему биту, если один символ занимает 8 бит? Ответ укажите в тысячах.

12. Выберите **все** верные утверждения по предыдущему заданию.

- 1) Каждый пиксель состоит из трёх цветовых каналов: красного, зелёного и синего (RGB).
- 2) Один символ текста занимает 8 бит памяти.
- 3) Если использовать замену по одному значащему биту на всю интенсивность кадра (то есть заменять во всех 8 битах канала), объём скрываемой информации увеличится в 8 раз.
- 4) Для одного символа потребуется 24 бита (по 8 бит на каждый цветовой канал пикселя).

13. Вычислить значение выражения: $1010010_2 + 10155_8 + 10BF_{16}$.

Результат записать в четверичной системе счисления.

14. 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 /).

Закодируйте слово **Ryazan** с помощью Base64.

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

	Значение	
	10	2
A	0	000000
B	1	000001
C	2	000010
D	3	000011
E	4	000100
F	5	000101
G	6	000110

	Значение	
	10	2
Q	16	010000
R	17	010001
S	18	010010
T	19	010011
U	20	010100
V	21	010101
W	22	010110

	Значение	
	10	2
g	32	100000
h	33	100001
i	34	100010
j	35	100011
k	36	100100
l	37	100101
m	38	100110

	Значение	
	10	2
w	48	110000
x	49	110001
y	50	110010
z	51	110011
0	52	110100
1	53	110101
2	54	110110

H	7	000111	X	23	010111	n	39	100111	3	55	110111
I	8	001000	Y	24	011000	o	40	101000	4	56	111000
J	9	001001	Z	25	011001	p	41	101001	5	57	111001
K	10	001010	a	26	011010	q	42	101010	6	58	111010
L	11	001011	b	27	011011	r	43	101011	7	59	111011
M	12	001100	c	28	011100	s	44	101100	8	60	111100
N	13	001101	d	29	011101	t	45	101101	9	61	111101
O	14	001110	e	30	011110	u	46	101110	+	62	111110
P	15	001111	f	31	011111	v	47	101111	/	63	111111

15. Выберите **все** верные утверждения об алгоритме Base64, который применялся в предыдущем задании.

Результат кодирования Base64 всегда короче оригинальных данных.

Base64 используется для кодирования двоичных данных в текстовый формат.

Base64 широко используется для кодирования изображений в формате PNG и JPEG в HTML.

Base64 является методом шифрования и обеспечивает безопасность данных.

16. Сопоставьте расширения файлов с описанием типов файлов, соответствующих этим расширениям.

Расширения файлов: .csr, .jar, .rules, .conf, .hash

Запрос на подпись сертификата, отправляется в удостоверяющий центр для получения подписанного сертификата.	.rules
Архивные файлы, содержащие Java code, могут содержать вредоносный код.	.csr
Файлы с правилами для систем обнаружения вторжений (IDS) и межсетевых экранов.	.hash
Файлы конфигурации для сетевых устройств и приложений, которые могут содержать настройки безопасности.	.jar
Файлы, содержащие хеш-суммы файлов. Используются для проверки целостности файлов.	.conf

17. Сопоставьте названия протоколов с их назначениями.

Названия протоколов: SSH, Kerberos, RADIUS, EAP, PGP.

Обеспечивает безопасный удаленный доступ к компьютеру или устройству. Шифрует весь трафик, включая пароли.	Kerberos
--	----------

Протокол сетевой аутентификации, использующий тикеты для подтверждения подлинности пользователей и служб.
Протокол аутентификации, авторизации и учета для пользователей, подключающихся к сети через сетевые устройства.
Фреймворк аутентификации, используемый в беспроводных сетях и других типах соединений, поддерживает различные методы аутентификации.
Протокол для шифрования и подписи электронной почты и других данных.

SSH
PGP
RADIUS
EAP

18. Установите соответствия между криптографическими средствами защиты информации и их назначениями.

Криптографические средства защиты: шифрование, электронная подпись, хеширование, криптографические протоколы.

Обеспечение конфиденциальности данных (предотвращение несанкционированного доступа к информации).
Подтверждение авторства (аутентификация отправителя и гарантия того, что сообщение не было подделано) и неотказуемость (отправитель не может отрицать факт отправки сообщения).
Обеспечение целостности данных (обнаружение изменений в информации после ее создания или передачи).
Обеспечение безопасной передачи данных по сети.

Шифрование
Криптографические протоколы
Электронная подпись
Хеширование

19. Установите соответствия между терминами, относящимися к персональным данным, и их определениями.

Термины, относящиеся к персональным данным: Персональные данные, субъект персональных данных, обработка персональных данных, оператор персональных данных, конфиденциальность персональных данных

Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).	Обработка персональных данных
Физическое лицо, к которому относятся персональные данные.	Оператор персональных данных
Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными.	Субъект персональных данных
Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.	Конфиденциальность персональных данных
Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.	Персональные данные

20. Установите соответствия между приложениями для защиты информации на смартфоне с их назначениями.

Приложение	Назначение
Антивирус	Шифрует данные на устройстве для предотвращения доступа
Менеджер паролей	Обнаруживает и удаляет вредоносное ПО
VPN	Автоматически заполняет и хранит сложные пароли
Приложение для резервного копирования	Создаёт защищённое подключение к интернету через удалённый

Программа шифрования данных

сервер
Создаёт копии важных данных для восстановления при утере

21. Вам представлен скриншот части вывода работы консольной утилиты `curl`, которая используется для выполнения HTTP-запросов. Рассмотрите скриншот и ответьте на вопросы.

1. Какой IP-адрес был использован для первичного подключения к серверу `rutube.ru`?
2. Какой протокол согласован для безопасного соединения (SSL/TLS)?
3. Сколько байтов данных содержит ответ сервера на *первый* запрос?
4. Сервер вернул статус-код 301. Что он обозначает? (выберите один верный вариант):
 - a) Status-код 301 означает, что запрашиваемый ресурс был перемещен на новый URI навсегда.
 - b) Status-код 301 означает, что требуется аутентификация для доступа к запрашиваемому ресурсу.
 - c) Status-код 301 означает, что сервер временно не может обработать запрос из-за перегрузки или обслуживания.
 - d) Status-код 301 означает, что произошла ошибка на стороне клиента, и запрос не может быть выполнен.

Запишите номер верного варианта ответа.


```

$ curl -v https://rutube.ru
* Trying 178.248.235.114:443...
* Connected to rutube.ru (178.248.235.114) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
* CAfile: /etc/ssl/certs/ca-certificates.crt
* Cpath: none
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* * TLSv1.3 (IN), TLS handshake, Server hello (2):
* * TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* * TLSv1.3 (IN), TLS handshake, Certificate (11):
* * TLSv1.3 (IN), TLS handshake, CERT verify (15):
* * TLSv1.3 (IN), TLS handshake, Finished (20):
* * TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* * TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_128_GCM_SHA256
* ALPN, server accepted h2
* Server certificate:
* subject: CN=*.rutube.ru
* start date: Jul 19 00:00:00 2025 GMT
* expire date: Aug 17 23:59:59 2025 GMT
* subjectAltName: host "rutube.ru" matched cert's «*.rutube.ru»
* issuer: CN=R3, O=Let's Encrypt, C=US
* SSL certificate verify ok.
> GET / HTTP/2
> Host: rutube.ru
> User-Agent: curl/7.81.0
> Accept: */*
>
< HTTP/2 301
< server: nginx
< date: Fri, 10 Sep 2025 12:34:56 MSK
< content-type: text/html
< content-length: 162
< location: https://rutube.ru/
< vary: Accept-Encoding

* Connection #0 to host rutube.ru left intact
* Closing connection 0
* TLSv1.3 (OUT), TLS alert, close notify (256):

```