ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТРУДУ (ТЕХНОЛОГИИ)

ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

ТЕОРЕТИЧЕСКИЙ ТУР

10 класс

Профиль «Информационная безопасность»

Уважаемый участник олимпиады!

Вам предстоит выполнить теоретические и кейс-задания.

Время выполнения заданий теоретического тура 3 астрономических часа (180 минут).

Часть предложенных Вам заданий может быть представлена в электронном виде. Для удобства работы с такими заданиями часть их условий перенесена на имеющийся у Вас черновик, на котором Вы можете делать любые записи, пометки, прорабатывать версии решения и иным образом активно работать с заданием. После завершения работы над заданиями черновик подлежит сдаче представителю организатора заключительного этапа олимпиады.

Выполнение заданий целесообразно организовать следующим образом:

– не спеша, внимательно прочитайте описательную часть задания;

– прочитайте часть задания, указывающую, что требуется определить и в какой форме ожидается ответ;

– определите наиболее верный и соответствующий требованиям задания ответ;

– отвечая на кейс-задание, обдумайте и сформулируйте конкретные ответы только на поставленные вопросы;

– если Вы выполняете задание, связанное с заполнением таблицы или схемы, 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.

Содержащий материалы заданий черновик теоретического тура входит в комплект материалов участника и подлежит сдаче по окончании работы.

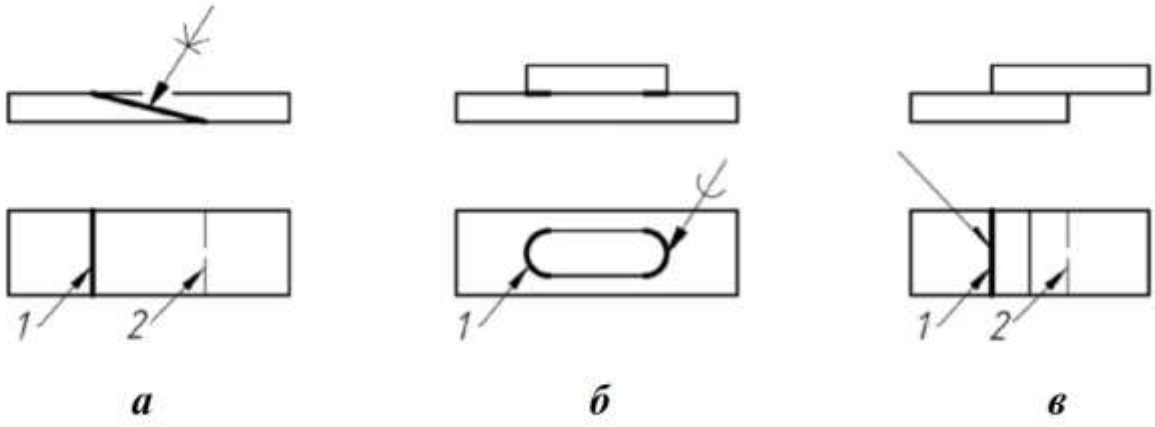
Максимальная оценка – 30 баллов (из них кейс-задание оценивается в 5 баллов).

Общая часть

1. (1 балл) Верны ли следующие утверждения?

№	Утверждение
1	LASER – аббревиатура, означающая усиление микроволн с помощью вынужденного излучения
2	LASER – аббревиатура, означающая усиление света с помощью вынужденного излучения
3	Прохоров Александр Михайлович и Басов Николай Геннадиевич (русские физики) в 1964 году получили Нобелевскую премию «за фундаментальные работы в области квантовой электроники, которые привели к созданию излучателей и усилителей на лазерно-мазерном принципе»
4	Чарльз Хард Таунс (американский физик) в 1964 году получил Нобелевскую премию «за фундаментальные работы в области квантовой электроники, которые привели к созданию излучателей и усилителей на лазерно-мазерном принципе»

2. (1 балл) Напишите название соединений и типы линий, представленных на чертеже? В чём основное назначение линии номер 1?



3. (1 балл) Установите соответствие термина в сфере беспилотных авиационных систем и его действию, которое совершается в БАС мультироторного типа. Ответ запишите в виде сочетания цифр и букв, например: 1А2Б3В

	Термин
1	Крен
2	Тангаж
3	Рыскание

	Действие
А	Линейная скорость полёта дрона (вперёд/назад)
Б	Повороты вокруг вертикальной оси (Z), по часовой или против часовой стрелки
В	Наклоны дрона на левый и правый бок

4. (0,5 балла) При генерации электричества ветрогенератором энергия переходит из одной формы в другую. Определите порядок преобразования энергетических форм во время работы ветряной турбины.

1 – механическая энергия вращения лопастей
2 – кинетическая энергия воздушного потока
3 – электрическая энергия, передаваемая в сеть
4 – электрическая энергия переменного тока
5 - электрическая энергия, запасенная в аккумуляторной батарее

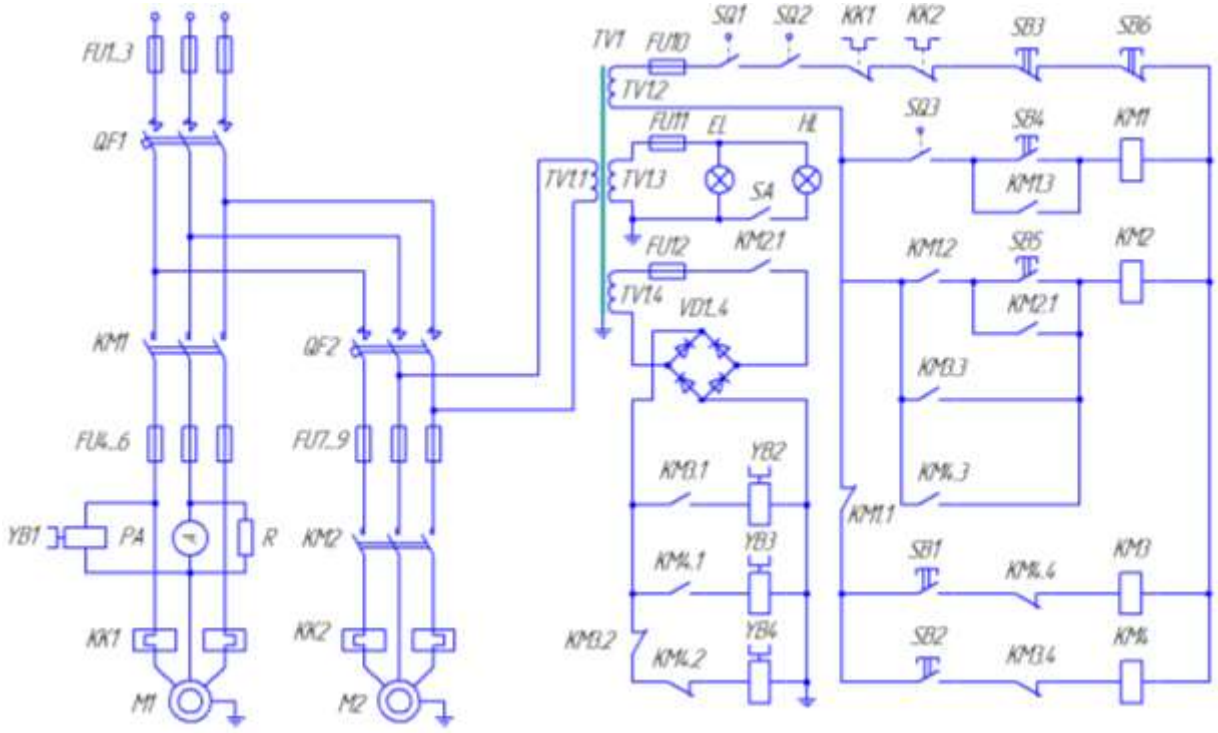
5. (1 балл) Активное и пассивное измерение загрязнения атмосферы – это два вида способов уменьшения загрязнения атмосферы вредными выбросами промышленных предприятий. Распределите способы уменьшения загрязнения атмосферы по эти двум видам.

1	активные
2	пассивные

А	строительство предприятий по проектам, прошедшим экологическую экспертизу
Б	размещение предприятий с учетом розы ветров
В	расположение промышленных предприятий с учетом рельефа местности
Г	создание санитарно-защитных зон в виде лесопосадок и парков
Д	повышение экологической безопасности сырья перед его применением
Е	рассеивание промышленных выбросов высокими дымовыми трубами

6. (1 балл) Предприниматель за первый год изготовил и реализовал продукцию в объеме 3 000 единиц на общую сумму 6 000 000 руб. при ее себестоимости 1 000 руб. за единицу. На следующий год себестоимость единицы продукции повысилась на 30 %. Какую прибыль получил предприниматель за два года, если за второй год своей деятельности он продал 4 000 единиц продукции по той же цене? Налоги не учитывайте. Ответ запишите в млн. руб.

7. (0,5 балла) На рисунке представлена электрическая принципиальная схема обрабатывающего станка. Определите, от какого напряжения питается цепь управления станка, и выберите правильный ответ:



а – 110 V
б – 220 V
в – 380 V

8. (2 балла) Петя создал необитаемый подводный аппарат с нулевой плавучестью. Задача аппарата собирать объекты со дна водоёма. Для этого необходимо НПА наклониться на угол 45 градусов по тангажу против часовой стрелки вокруг некоторого центра. Помогите Пете с расчётами, хватит ли тяги движителей для удержания угла? Выберите все правильные утверждения. Ответ запишите в виде последовательности цифр по возрастанию без пробелов, например, 1234.

1) Тяги хватит.
2) Тяги не хватит.
3) Если поменять местами центр плавучести и центр тяжести, не поменяется ситуация с удержанием угла.
4) Если поменять местами центр плавучести и центр тяжести, то это позволит удерживать заданный угол.
5) Если сместить движители на высоту центра тяжести, то тяги не хватит для удержания угла.
6) Если сместить движители на высоту центра плавучести, то тяги станет хватать для удержания угла.

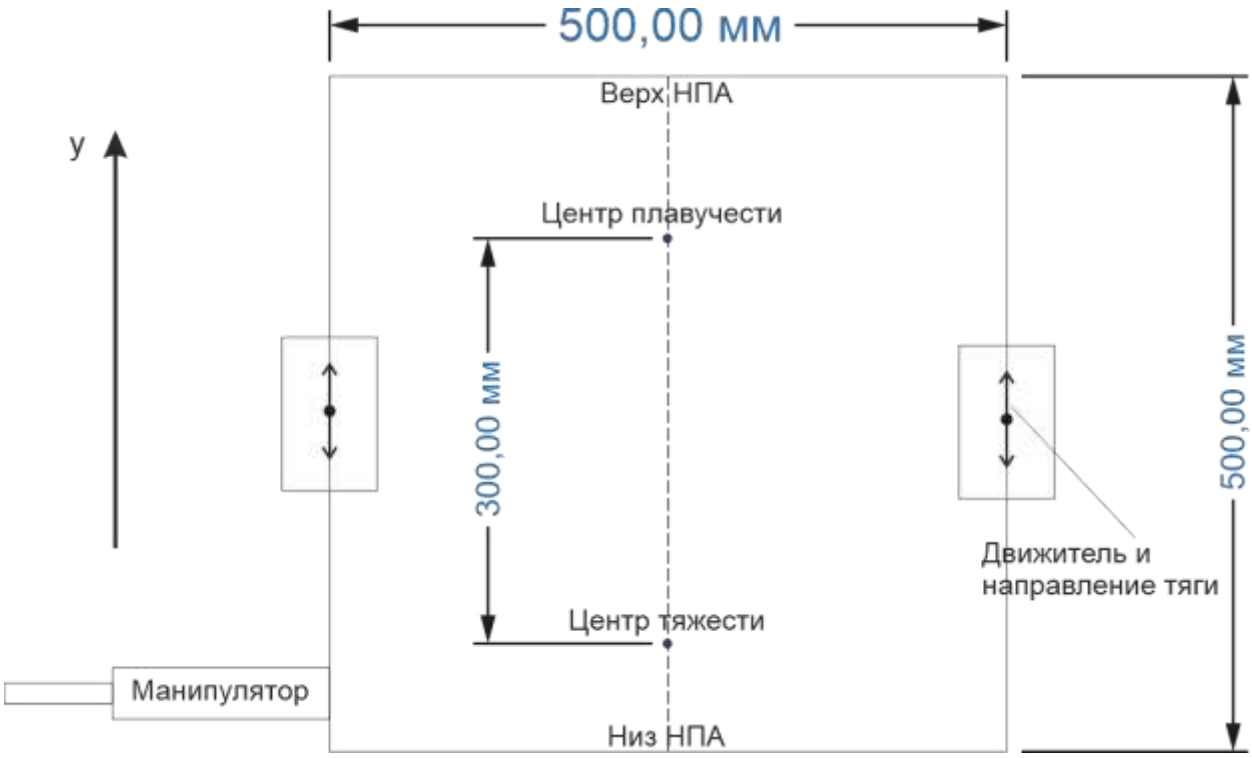


Рис. 1. Необитаемый подводный аппарат

Масса НПА - 10 кг.

Движитель. Тяга в прямом направлении (совпадает с направлением оси y): 0,2 кгс (при номинальном напряжении). Тяга при реверсе: 0,15 кгс (при номинальном напряжении).

1 килограмм-сила (кгс) равен 9,80665 ньютона (Н).

Центр плавучести – это местоположение внутри твердого объекта, погруженного в жидкость, где сумма всех сил давления распределяется в направлении, противоположном направлению силы тяжести.

Специальная часть

В компании **«X»** произошел инцидент: несколько подписанных документов вызвали подозрения у отдела информационной безопасности. Каждый документ был подписан цифровой подписью на основе схемы RSA, то есть у каждого пользователя имеется ключевая пара из секретного ключа, используемого для подписывания сообщений, и открытого ключа, который нужен для проверки подписей.

Данная схема реализована следующим образом:

1) Компания выбрала два простых числа – p и q. Далее вычисляется их произведение N = p*q.

2) Для этого произведения вычисляется значения функции Эйлера, $\varphi(n) = (p - 1)(q - 1)$.
3) Выбирается натуральное число e, большее 1 и меньшее $\varphi(n)$, не имеющее общих делителей (взаимно простое) с $\varphi(n)$.
4) Для выработки подписи S сообщения m необходимо вычислить остаток от деления числа m^d на n (или найти m^d по модулю n, записывается (mod n)), где d – секретная степень, вычисленная так, чтобы выполнялось условие: $d * e \equiv 1 \pmod{\varphi(n)}$, то есть произведение e и d равнялось 1 по модулю значения $\varphi(n)$. Число d вместе с исходными p и q хранится в секрете и составляет секретный ключ.
5) Служба безопасности для проверки подписи сообщения m, являющегося целым числом от 1 до n, должна возвести его подписанное значение m^d в степень e так же по модулю n. Пара (e, n) составляет открытый ключ, служащий для проверки подписи.

Известно, что p = 11, q = 17, а e = 7.

9. Найдите значение d секретного ключа. (1 балл)
10. У компании есть список документов, которые вызывают подозрения. Для каждого из них даны m и вычисленные подписи S:

- Документ A: M = 12, S = 104
- Документ B: M = 9, S = 36
- Документ C: M = 68, S = 85
- Документ D: M = 14, S = 92
- Документ E: M = 9, S = 81
- Документ F: M = 30, S = 30
- Документ G: M = 148, S = 92

На основе открытого ключа и вычисленного в пункте 1 значения d проверьте корректность подписи, вычислив M’. Укажите все документы, для которых вычисленное значение M’ ≠ M. *(1 балл)*

11. Найдите такое минимальное натуральное значение d’, для которого выполняется $d' * e \equiv 1 \pmod{\varphi(n)}$, но $d' > \varphi(n)$. (1 балл)

Системный администратор некоторой компании, занимающийся также и вопросами безопасности, прочитал, что хранение паролей на сервере в открытом виде небезопасно. Решение с функциями хэширования показалось ему слишком сложным, поэтому он решил поступить иначе. На самом сервере он задал

регулярное выражение и далее создал и раздал пользователям пароли, которые этому регулярному выражению соответствовали.

Регулярные выражения – это формальный язык задания шаблонов, по которым можно искать в тексте некоторые подстроки. Например, можно искать фрагмент, являющийся адресом электронной почты (зная, что это несколько символов, затем символ @, затем доменное имя, состоящее из 2 частей, разделенных точкой), телефонным номером (последовательность из определенного числа цифр, причем при известной стране можно указать в шаблоне соответствующий код), номером банковской карты, адресом и т. п.

Регулярное выражение, использованное системным администратором, может включать следующие фрагменты (условно назовем их блоками):

- Один символ из некоторого множества заданных. Например, выбор из букв “a”, “b” или “c”. Совпадением будет считаться любая из этих букв. В регулярном выражении такой выбор записывается так: [ab]
- Один любой символ кроме заданных. Например, любой символ кроме букв “a” и “b”. Такой выбор записывается так: [^ab]
- Любой одиночный символ. Соответствующая запись – символ точки: «.» (без кавычек).
- Один из двух символов – например, “a” или “b”. Соответствующая запись: a|b.
- Необязательный символ (может присутствовать или отсутстовать). Соответствующая запись: a? – ровно один символ “a” или его отсутствие.
- Несколько одинаковых символов, число которых попадает в заданный диапазон. Например, “aaa”. Соответствующая запись: a{1,3} – от 1 до 3 символов “a”
- Любая одна цифра. Соответствующая запись: \d

В случае, если в подстроке нужно искать какой-то символ, являющийся частью описания блока (например, открывающаяся и закрывающаяся скобка, символ «^»), то перед ними ставят символ «\». В этом случае они не воспринимаются как часть описания блока. Некоторые блоки требуют заключения в круглые скобки, чтобы считаться частью общего шаблона.

Например, регулярное выражение Hello, [Ww]orld[!?] означает

- “Hello, “ — фиксированный фрагмент текста,

- [Ww] — буква “W” или “w”,
- “orld” — фиксированный фрагмент текста,
- [!?] — строка должна заканчиваться либо “!”, либо “?”

Этому шаблону соответствуют следующие строки:

- Hello, World!
- Hello, world!
- Hello, World?
- Hello, world?

Но не соответствует

- Hello, World$ (последний символ не входит в набор [!?])

Тогда, например, задав регулярное выражение (здесь отдельные блоки выделены разными цветами)

[abcde](\#|\$)[fgh](\(|\))\dg?Run

администратор может создать для пользователей пароли

- a#g(1gRun
- c$g)7Run
- e#h)4gRun
- b$f)9gRun

и другие, соответствующие тому же шаблону.

Нарушитель узнал, что на сервере аутентификация происходит на основе некоторого (недавно измененного администратором) шаблона. Ему также удалось приобрести несколько ранее использовавшихся паролей:

- ap$+bbxZZ!
- iq%*bzZZZ?
- or£^bbyZZ%
- ep&+bxZZ!

- us$*bbyZZ?
- is£^bbzZZ{
- aq$+bxZZZ!
- oq&^bbxZZ%
- ut%*bbyZZ?
- es$+bzZZ}

Сейчас эти пароли уже признаны администратором скомпрометированными и заблокированы. Вместе с каждым из них блокируются и все пароли, расстояние Левенштейна до которых не превышает 2.

Расстояние Левенштейна (известна также как редакторская метрика) – мера, показывающая насколько отличаются две строки. Растояние равно минимальному числу операций, которые нужно сделать, чтобы превратить одну строку в другую. Есть три возможных операции:

• Замена

• Вставка

• Удаление

Например, слова «КОТ» и «КОД» имеют расстояние Левенштейна равное 1, так как для преобразования одного слова в другой требуется одна операция замены «Т» на «Д».

Слова «КОТ» и «КРОТ» так же имеют расстояние Левенштейна равное 1, потому что нужно применить только одну операцию вставки буквы «Р».

Для слов «СЛОНЫ» и «СТОЛ» потребуется больше операций:

• Операция замены «Л» на «Т»

• Операция замены «Н» на «Л»

• Операция удаления «Ы»

Таким образом, расстояние Левенштейна между этими словами – 3.

Операция перестановки символов не предусмотрена. Чтобы превратить строку «ТО» в «ОТ» нужно применить 2 операции – удаления и вставки или 2 операции замены.

12. Определите количество блоков в регулярном выражении, которому соответствуют приобретенные нарушителем пароли (считайте блоками фрагменты регулярного выражения, проводящие одну проверку). (0,5 балла)
13. Установите, сколько различных паролей, соответствующих действующему шаблону, блокирует администратор вместе с каждым из скомпрометированных. (1 балл)
14. Определите расстояние Левенштейна между строками «ПРОГРЕСС» и «ПАРОЛЬ» (1 балла)
15. Составьте любой пароль, с помощью которого возможно авторизоваться в системе при действующем шаблоне. (1,5 балла)

Матрица — это прямоугольная таблица чисел, расположенных в строках и столбцах. Матрица обычно обозначается большой буквой и имеет размер m × n, где m — количество строк, а n — количество столбцов. Например, матрица A размера 2 × 3 выглядит так:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}$$

Вектор — это упорядоченный набор из n чисел. Длиной вектора называется число n. Например

$$a = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

— вектор длины 2. Таким образом, под вектором можно понимать мат-

рицу размера n × 1.

Единичная матрица — матрица с единицами в ячейках с одинаковыми индексами и нулями в остальных. Пример единичной матрицы 2 × 2:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Обратимая матрица — это квадратная матрица A размера n × n, для которой существует другая матрица B такая, что произведение A × B = B × A = I, где I — это единичная матрица. Если такая матрица B существует, то A называется обратимой, а B — обратной к A.

Умножение матриц — это операция, при которой две матрицы A и B размера n × m и m × k соответственно (з умножаются друг на друга, и результатом является новая матрица C размера n × k (для этого важно, чтобы «соседние» размеры матриц (число столбцов в первой матрице и число строк во второй, равное m в данном примере) совпадали – только в этом случае их можно умножать). Каждый элемент c_{ij} матрицы C вычисляется как сумма произведений элементов i-й строки матрицы A на соответствующие элементы j-го столбца матрицы B:

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdot\cdot\cdot + a_{in}b_{nj}$$

Например, для матрицы A размера 2 × 2 и B размера 2 × 1:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} \\ b_{21} \end{pmatrix}, \quad C = A \times B = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} \\ a_{21}b_{11} + a_{22}b_{21} \end{pmatrix}$$

Шифр Хилла – шифр замены, в котором последовательность символов длины n заменяется на последовательность той же длины n. Каждой букве алфавита сопоставляется число по модулю 31 (будем считать, что и=й, е=ё). Блок из n букв открытого текста рассматривается как вектор длины n и умножается по модулю 31 на матрицу размера n×n. Элементы данной матрицы являются ключом. Буквы открытого текста переводятся в числа, согласно таблице. Аналогично числа, полученные в результате шифрования, преобразуются в буквы. В модифицированной версии шифра Хилла к полученным после умножения значениям добавляют вектор

$$b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix},$$

который является частью ключа и, соответственно, также хранится в секрете.

Вам дана следующая таблица соответствий:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф
9	30	29	17	20	21	5	12	2	3	0	25	14	19	28	10	7	13	26	24

Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
23	18	15	6	8	16	4	11	1	27	22

Известно, что при шифровании использовались блоки дины n = 2. Это означает, что процесс шифрования можно представить как умножение матриц следующим образом:

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \pmod{31}$$

где mod 31 – взятие числа «по модулю 31», то есть нахождение остатка от деления каждого значени на 31, а

$$P = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \text{ и } C = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

— векторы длины 2, представляющие открытый текст и зашифрованный текст соответственно, K — матрица 2 × 2, представляющая ключ шифрования, b – добавляемый вектор.

16. Вы смогли перехватить зашифрованный текст ХАБЯПД, ключ

$$K = \begin{pmatrix} 1 & 5 \\ 6 & 4 \end{pmatrix}, \quad b = \begin{pmatrix} 7 \\ 18 \end{pmatrix}$$

Найдите исходный текст. *(1,5 балла)*.

17. Зная открытый текст из предыдущего задания и новый перехваченный шифртекст ХЧХЪГЯ, восстановите ключ. (2 балла)

18. Сколько необходимо перехватить попарно-различных пар биграмм (пар блоков букв длины 2 открытого текста и соответствующих им блоков шифртекста), чтобы гарантированно восстановить ключ? (1,5 балла)

Кодирование – это отображение $\varphi: I \to B$ из множества информационных слов I в множество двоичных последовательностей B.

Образ $\varphi(i)$ информационного слова $i \in I$ называется **кодовым словом**.

Множество всех кодовых слов, соответствующих информационным словам из множества I называется **кодом**.

Длина кодового слова – это длина двоичной последовательности, которой оно является.

Блочный код - код, в котором все кодовые слова имеют одинаковую длину.

Расстоянием Хэмминга $\boldsymbol{d(x,y)}$ между двумя двоичными последовательностями одинаковой длины x и y называется число позиций, в которых они различаются.

Пример: $x = 11101$, $y = 01100$, $d(x, y) = 2$, кодовые слова различаются в двух двоичных позициях.

Декодирование по методу максимального правдоподобия – поиск среди всех исходных кодовых слов того, которое имеет минимальное расстояние Хемминга с искаженным.

Пример:

Искаженное кодовое слово 001.

Множество кодовых слов: {000, 111}.

Расстояние Хемминга с первым кодовым словом равно 1, расстояние Хемминга со вторым кодовым словом равно 2. Значит, в качестве исправленного выбирается первое кодовое слово.

Блочный код может быть построен так, чтобы при декодировании по методу максимального правдоподобия, получалось обнаруживать и исправлять ошибки (искажения битов), которые происходят при передаче кодовых слов по каналу связи.

Код обнаруживает ошибку, если при декодировании подается сигнал об отличии принятой двоичной последовательности от отправленного по каналу связи кодового слова (то есть, если это искаженное кодовое слово не является элементом множества кодовых слов).

Код исправляет ошибку, если при декодировании двоичной последовательности (искаженного кодового слова) удается верно установить отправленное кодовое слово.

Кратность обнаруживаемых ошибок T – это максимальное количество ошибок (искаженных бит) в кодовом слове, которое гарантированно может обнаружить код (то есть вне зависимости от того какое изначально было кодовое слово и вне зависимости от тех позиций, в которых произошли искажения).

Пример: код {00, 01, 10, 11} не обнаруживает ни одной ошибки, а код {00, 11} обнаруживает одну ошибку.

Кратность исправляемых ошибок t – это максимальное количество ошибок (искаженных бит) в кодовом слове, которое гарантированно может исправить данный код (то есть вне зависимости от того какое изначально было кодовое слово и вне зависимости от тех позиций, в которых произошли искажения).

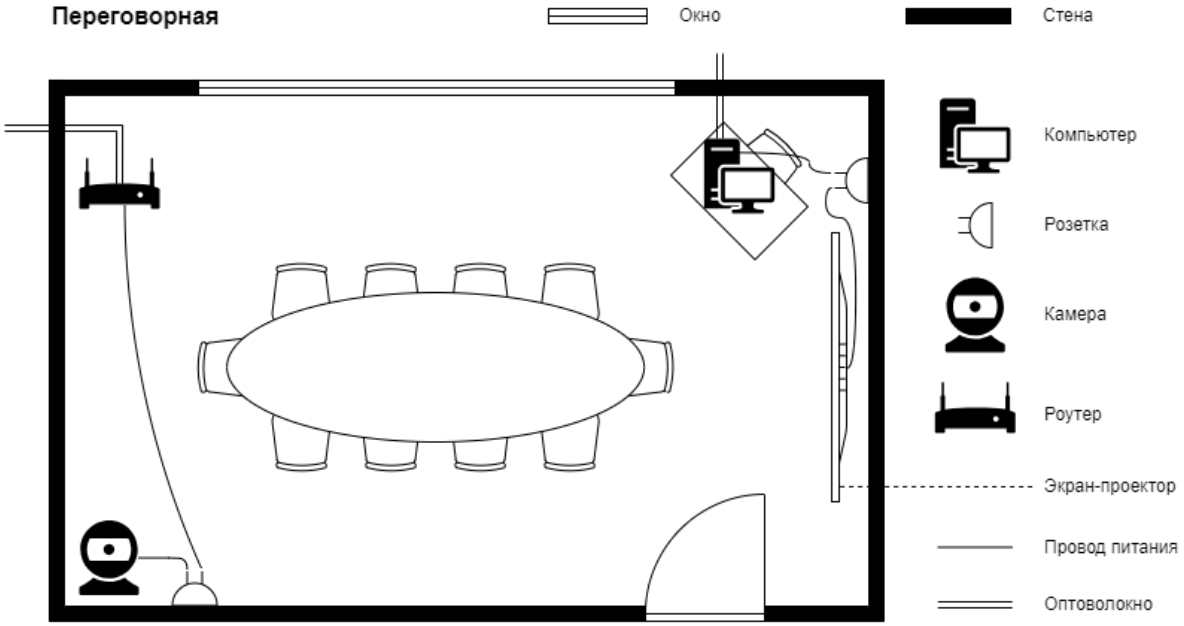
Пример: код {00, 01, 10, 11} не исправляет ни одной ошибки, а код {000, 111} исправляет одну ошибку.

19. Известно, что блочный код содержит 17 кодовых слов и имеет кратность обнаруживаемых ошибок 1. Какая минимальная длина кодовых слов возможна в таком случае? (2 балла)
20. Для дальнейшей работы необходимо, чтобы кратность исправляемых ошибок была 1. Чтобы длина кодовых слов не была слишком большой, число кодовых слов сократили до 4. Вам известны два кодовых слова: 00000 и 11011. Сколько существует различных кодов, содержащих эти кодовые слова и подходящих под условие?
Комментарий: коды являются различными, если у них отличаются множества кодовых слов, из которых они состоят. *(2 балла)*

21. Был выбран один из кодов из предыдущего задания. Какую максимальную кратность обнаруживаемых ошибок он может иметь? (1 балл)

Кейс-задание

22. Перед Вами план переговорной комнаты в офисе крупной компании.



Вам поручено оценить, какие объекты в помещении могут быть использованы нарушителями для организации утечки информации по техническим каналам утечки информации (ТКУИ). Укажите, какие объекты, находящиеся в помещении, могут быть использованы для создания таких каналов, какие устройства перехвата информации может использовать нарушитель, а также предложите меры защиты от утечек по такому каналу. Для получения максимального балла рассмотрите не менее 5 различных по принципу формирования ТКУИ с соответствующими объектами, устройствами перехвата и мерами защиты. *(5 баллов)*