ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТЕХНОЛОГИИ

ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

ТЕОРЕТИЧЕСКИЙ ТУР

9 класс

Профиль «Информационная безопасность»

Уважаемый участник олимпиады!

Вам предстоит выполнить теоретические и кейс-задания.

Время выполнения заданий теоретического тура 2,5 астрономических часа (150 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.

Кейс-задание выдано Вам на отдельном листе, содержащем условие и место для представления ответа. В данном задании при оценке учитывается решение, которое для получения максимального балла требуется оформить разборчиво, полно для понимания хода решения, а также в понятном для членов жюри порядке изложения, по возможности избегая значительных исправлений.

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 – 25 баллов (из них кейс-задание оценивается в 5 баллов).

Общая часть

1. Представьте, что Вы выполняете сложный технологический проект и Вам нужно посчитать энергозатраты при его серийном производстве.
Условия следующие:

1 кВт/ч электроэнергии стоит 5,54 руб.

- Лазерно-гравировальный станок имеет энергопотребление 400 Вт в час и выжигает лицевую панель 30 минут.
- 3D принтер работает 3 часа, печатая основной корпус, потребляя 200 Вт за один час.
- Паяльная станция имеет энергопотребление 100 Вт за один час и работает ровно один час при пайке схемы.
- Компьютер используется 10 минут при прошивке микроконтроллера и имеет энергопотребление 600 Вт в час.

Какую сумму денежных средств необходимо заложить в раздел «Энергозатраты на выполнение всех операций при производстве одной серийной единицы изделия»? Ответ дайте в рублях. В ответе запишите целое число.

2. В неисправном электроприборе произошло короткое замыкание. Какое защитное устройство отключит питание?

а. – устройство дифференциального тока (УДТ) с номинальным током утечки 30 мА

б. – автоматический выключатель С16

в. – автоматический выключатель, управляемый дифференциальным током, со встроенной защитой от сверхтока (АВДТ) С25 с номинальным током утечки 100 мА, установленный на вводе

г. – ничего из вышеперечисленного

д. – всё из вышеперечисленного

3. Впишите во второй столбик наименования отраслей человеческой деятельности, к которым относятся указанные профессии.

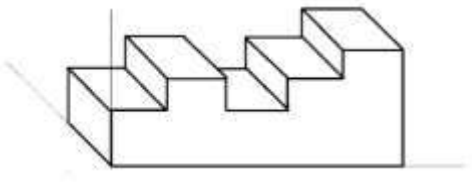
Профессии	**Отрасли человеческой деятельности**
проектировщик доступной среды; архитектор энергонулевых домов; управляющий жизненным циклом городских объектов	1 –
молекулярный диетолог; клинический биоинформатик; фармакологический эколог	2 –
проектировщик дирижаблей; регулировщик дронов; разработчик интеллектуальных диспетчерских систем	3 –

4. Поставьте правильное соответствие между изобретением, его автором и

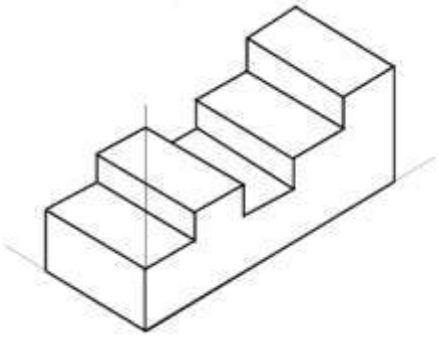
годом, когда оно было сделано, указав в таблице арабскую и римскую цифры:

А	Александр Белл	1	Радио	I	1960 г.
Б	Томас Эдисон	2	Лазер	II	1876 г.
В	Теодор Нейман	3	Телефон	III	1895 г.
Г	Александр Попов	4	Электрическая лампочка	IV	1879 г.

5. Соотнесите названия аксонометрических проекций с их изображением.



а



б

1. Прямоугольная изометрическая проекция
2. Косоугольная фронтальная диметрическая проекция

Специальная часть

В организации N для обеспечения безопасности хранящихся кодов товаров, состоящих только из строчных букв русского алфавита (всего 33 символа), придумали функцию хеширования, которая работает по следующему алгоритму:

1. На вход подается строка P длины L, которая разбивается на 2 части P_1 и P_2 так, что $P = \overline{P_1 P_2}$, где $P_1 = \overline{p_1 \dots p_{\lfloor L/2 \rfloor}}, P_2 = \overline{p_{\lfloor L/2 \rfloor + 1} \dots p_L}$.
   Здесь черта над несколькими элементами ознаает, что эти элементы, представляющие собой строки, должны быть сцеплены в единую строку. Например, если a = «при», b = «мер», то ab = «пример»
2. Вычисляется значение

$$Hash_{10}(P = \overline{P_1 P_2}) = 2^{3 \cdot L} \cdot ((L \cdot 2)^{222} \cdot \sum_{i=1}^{\lfloor L/2 \rfloor} p_i + (L+4)^{222} \cdot \sum_{i=\lfloor L/2 \rfloor + 1}^{L} p_i)(mod m)$$

где $\sum_{i=a}^{b} p_i$ обозначает сумму букв пароля, начиная с позиции a, заканчивая позицией b (обе границы включаются), по их номерам в русском алфавите (от 1 до 33 включительно).

Например, для $P = \overline{бв}$ сумма вычисляется следующим образом:

$\sum_{i=1}^{2} p_i = 2 + 3 = 5$;

$\lfloor L/2 \rfloor$ обозначает целую часть от деления L на 2;

$(mod m)$ обозначает взятие остатка от деления полученного значения на m.

3. Полученное в шаге 2 значение переводится в двоичный код $Hash$ длины 8 с добавлением ведущих нулей при необходимости. Например, $Hash_{10} = 6_{10} \Rightarrow Hash = 00000110_2$.

Полагая $m = 227$ - простое число, выполните следующие **задания**:

6. Выберите из предложенных значений те, которые невозможно получить в результатет вычисления описанной выше хеш-функции: (0,5 балла)

1) 10001000	4) 11100000	7) 10000011
2) 11101111	5) 10110100	8) 11100101
3) 00011000	6) 11101010	9) 00101011

7. Вычислите по алгоритму, приведенному выше, значение хеш-функции для строки «всош». (1,5 балла)
8. Найдите такую строку P наименьшей длины, что $P_1 = P_2$, P_1 не содержит символов «ь» и «ъ», в P_2 символы не повторяются и $Hash(P) = 00000000$. В случае, если таких строк несколько, в качестве ответа приведите **наибольшую** в лексикографическом порядке (по алфавиту). (2 балла)

Специалист по информационной безопасности компании N в январе 2024 года выпустил новые правила использования парольной аутентификации, в которой описаны следующие требования:

1. Пароль должен иметь длину не менее 10 символов, состоять только из символов русского алфавита (33 буквы) или цифр, при этом обязательно содержать:
   1. Хотя бы одну букву *«ё»* в любом регистре;
   2. Не менее двух заглавных букв, при этом все заглавные буквы должны быть различными;

3. Не менее трех цифр, причем цифры в пароле не могут стоять рядом друг с другом.
2. Сотрудник обязан менять пароль 1 числа каждого месяца, причем задавать один из ранее использованных паролей недопустимо.
3. Для исключения возможности подбора пароля методом перебора система автоматически отключает возможность аутентификации данного пользователя на 10 секунд при вводе пяти неверных паролей подряд.

Чтобы не забывать пароли, но при этом следовать требованиям, менеджер Алиса каждый месяц меняет один случайный символ пароля и устанавливает получившуюся комбинацию символов в качестве нового. 1 февраля 2024 года она установила свой первый пароль *«йцУ9К2ё7н4»*.

В данный момент злоумышленник Иван, знающий новые правила аутентификации, используемые в компании N, пытается взломать пароль Алисы, реализуя следующие этапы атаки:

1. Используя социальную инженерию на протяжении ровно восьми часов, Иван компрометирует февральский пароль Алисы и узнаёт, что в марте она изменила одну из цифр на символ *«щ»;*
2. После получения информации о предыдущих паролях Иван перебирает все возможные варианты нового пароля со скоростью 1 пароль в секунду.

Задания:

9. На какое количество символов Алиса могла заменить символ *«К»* при создании апрельского пароля? (0,5 балла)
10. Сколько секунд *в худшем случае* потратит Иван на исполнение всех этапов своей атаки? (2 балла)
11. В каком самом раннем месяце у Алисы может получиться пароль, содержащий подряд идущие символы *«КрИпТо»?* В качестве ответа укажите номер месяца и год. (1,5 балла)

Для разграничения доступа к данным клиентов в банке N используется сочетание ролевой и дискреционной моделей. За счет этого удается предоставлять менеджерам, работающим с клиентами банка, доступ только к данным определенных клиентов (индивидуально настраиваемый набор для каждого менеджера). Роль, содержащая явно указанные права доступа для всех объектов, присваивается всем сотрудникам банка, все сотрудники, работающие с клиентами имеют роль «Менеджер». При этом некоторым из них могут отдельно

устанавливаться права доступа, связанные с их идентификаторами. При запросе на доступ к объекту проверяются права доступа роли и наличие прав идентификатора. Если такие права не заданы, применяются только права роли, в противном случае учитываются оба значения права доступа.

Задания:

12. Определите, какие права – роли или идентификатора пользователя – должны иметь приоритет для реализации описанного разграничения доступа, если для принятия решения требуется однозначно выбрать одно из двух (возможно, противоречащих друг другу) установленных значений (0,5 балла)

    1. Роли
    2. Идентификатора

13. Пусть при наличии заданных прав идентификатора в случае запроса на доступ к объекту запрашиваются оба значения прав. Определите, при помощи какой логической функции 2 переменных следует принимать решение о предоставлении доступа или отказе в нем для реализации описанного разграничения доступа в рамках всей организации (не только для менеджеров). Заполните таблицу истинности этой функции. Наличию права (разрешенному доступу) соответствует «1», отсутствию права (явному запрету) соответствует «0». (0,5 балла балл)

роль	id	доступ
0	0	
0	1	
1	0	
1	1	

14. Петр имеет роль «Менеджер» и набор прав доступа для 8 клиентов (№№ с 1 до 8), который в 16-ричной системе счисления задан как E7. Определите, может ли он получить доступ к данным клиентов №2 и 4. (0,5 балла)

    1. Имеет доступ к данным обоих клиентов
    2. Имеет доступ к данным только клиента №2
    3. Имеет доступ к данным только клиента №4

4. Не имеет доступа к данным указанных клиентов

15. Для доступа к файлам бухгалтерии используется более строгий принцип определения права доступа. Обязательно наличие права роли, которое – при наличии заданных прав идентификатора – должно ими подтверждаться. Права роли «Бухгалтер» на доступ к 8 объектам (№№ с 1 до 8) заданы в 16-ричной системе счисления как DB. Права идентификатора бухгалтера Петрова аналогично заданы как 7E. Перечислите номера объектов, к которым может получить доступ Петров. (1 балл)

16. Для бухгалтера Сидорова требуется обеспечить доступ к объектам, являющимся файлами бухгалтерии, с номерами 3, 5 и 8. Определите, можно ли обеспечить такой доступ в рамках роли «Бухгалтер», права для которой заданы в 16-ричной системе счисления как DB (0,5 балла).

- Да
- Нет

17. Укажите в шестнадцатеричном виде набор прав идентификатора Сидорова, необходимый для обеспечения ему доступа только к указанным выше объектам с номерами 3, 5 и 8 (нумерация объектов слева направо, т.е. старший бит соответствует объекту №1, младший – объекту №8). (1 балл)

Помехоустойчивое кодирование - процесс преобразования информации, предоставляющий возможность обнаружить и исправить ошибки, возникающие при передаче информации по каналам передачи данных. Это возможно благодаря добавлению к исходной последовательности специально структурированных дополнительных бит. **Декодирование** – восстановление исходной последовательности.

Помехоустойчивый код – код, предназначенный для обнаружения и исправления ошибок

Блочный (n,k)-код – код, который k-разрядной исходной двоичной последовательности (информационное слово) ставит в однозначное соответствие n-разрядную кодовую двоичную последовательность (кодовое слово). Пример: (8,4)-код: информационное слово – 0110 (4 бита), кодовое слово – 01101100 (8 бит)

Кратность исправляемых ошибок t – это максимальное количество ошибок (искаженных бит) в кодовом слове, которое может исправить данный код

Кратность обнаруживаемых ошибок T – это максимальное количество ошибок (искаженных бит) в кодовом слове, которое может обнаружить код

Расстояние Хемминга d – количество позиций элементов двух кодовых слов, в которых они не совпадают. Пример: одно кодовое слово 101101, второе кодовое слово – 011010. d=5, кодовые слова различаются в пяти двоичных позициях.

Декодирование методом максимального правдоподобия (метод сопоставления) – поиск среди всех исходных кодовых слов того, которое имеет минимальное расстояние Хемминга с искаженным. Пример: искаженное кодовое слово 0000001. Исходные кодовые слова 0000000, 1010001. Расстояние Хемминга с первым кодовым словом равно 1, расстояние Хемминга со вторым кодовым словом равно 2. Значит, в качестве исправленного выбирается первое кодовое слово.

Код с проверкой на четность – код, добавляющий к информационной последовательности бит чётности. Бит чётности вычисляется как сумма по модулю 2 всех бит исходного слова. Позволяет обнаружить одну ошибку. Пример: исходное слово 0110100. Сумма по модулю 2 равна одному, поэтому кодовое слово 01101001. Исходное кодовое слово 0010100. Сумма по модулю 2 равна нулю, поэтому кодовое слово 00101000.

Код Хемминга(7,4) – блочный код исправляющий одну или обнаруживающий две битовые ошибки. Построение кодового слова C осуществляется по правилу: C=(i1, i2, i3, i4, p1, p2, p3), где i1, i2, i3, i4 – биты информационного четырёхбитового слова, p1, p2, p3 – проверочные символы, равные сумме по модулю 2 исходных бит. p1 = i1+i2+i4, p2 = i1+i3+i4, p3 = i2+i3+i4. Пример: информационное слово = 0110. Кодовое слово C=0110110.

Пусть в системе связи компании для помехоустойчивого кодирования используется код Хемминга(7,4) с добавлением дополнительного бита чётности, полученного из кодового слова. Таким образом, каждые 4 бита исходной последовательности кодируются 8 битами (последовательно строится код Хемминга, а затем добавляется бит чётности). Символами исходного алфавита являются латинские буквы в верхнем и нижнем регистрах и цифры из таблицы ASCII (каждый символ занимает один байт). Таблица приведена в приложении.

Задания:

18. Закодировать текст «dQw». Ответ привести в виде двоичного кода, представленного в шестнадцатеричной форме. Например, «ab0f5». (1 балл)

19. Декодировать полученный по системе связи двоичный код «4ac2629b3926», представленный в шестнадцатеричной форме. Гарантируется, что в каждом кодовом слове после передачи по каналу связи произошло не более одной ошибки. Ответ привести в виде текста в кодировке ASCII. Например, «t5F» (1 балл)

20. Дан полученный по системе связи двоичный код «4ac80cfe723860217cef7373», представленный в шестнадцатеричной форме. Гарантируется, что в каждом кодовом слове после передачи по каналу связи произошло не более двух ошибок. Посчитать, сколько блоков было передано без искажений, сколько блоков было исправлено (одна ошибка в блоке), в скольких блоках можно только обнаружить ошибку, но не исправить (2 ошибки в блоке). Перечислите полученные числа без пробелов. Например, без искажений – 3, исправлено – 10, обнаружена ошибка – 5. Тогда в качестве ответа необходимо написать 3105. (1 балл)

Шифр, известный как “Два квадрата”, заключается в замене пар символов, стоящих один за другим, на пары символов того же алфавита. Замена происходит по следующему принципу: символы алфавита вносятся в две квадратные или прямоугольные таблицы в случайном порядке, например, так:

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

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

Далее в таблицах отыскиваются символы шифруемой пары: первая буква отыскивается в левой таблице, вторая – в правой. Зашифрование пары символов происходит по следующим правилам:

Если они стоят в разных строках и столбцах, то для определения символов замены требуется мысленно расположить символы открытого текста в противоположных углах прямоугольника, так, чтобы соединяющий их отрезок являлся его диагональю. Символы замены должны находиться в других углах прямоугольника, а записать их нужно, двигаясь по другой диагонали из правой таблицы в левую. Например, «ЗУ» – «ВЩ», «ОТ» – «.Е».

Если символы шифруемой пары стоят в одной строке, то для замены берется пара символов, расположенных в той же строке, но номера столбцов обмениваются местами. То есть, если первая буква стоит в столбце №2 левой таблицы, а вторая – в столбце №4 правой таблицы, то для замены нужно взять буквы той же строки из столбца №2 правой таблицы и столбца №4 левой таблицы. Например, «СВ» зашифровывается парой «ЛБ», «ЗЛ» – «ОС», «УМ» – «ЯП».

Если координаты символов шифруемой пары в соответствующих таблицах совпадают, то для получения пары замены символы обмениваются местами. Например, «ЗО» – «ОЗ», «ЖИ» – «ИЖ».

Обратите внимание, что символы пробела (или «_»), точки и запятой являются полноправными символами алфавита, учитываемыми в открытом тексте и используемыми в шифртексте.

В распоряжении криптоаналитика оказался значительный объем открытых текстов и соответствующих им зашифрованных текстов, полученных одним и тем же шифром, что можно представить в виде двух бесконечных последовательностей символов, в которых могут встретиться любые интересующие комбинации. В такой ситуации криптоаналитики стремятся проверить, мог ли быть использован именно шифр «Два квадрата». Для проверки этого в открытом и зашифрованном текстах ищут некоторые комбинации символов, характерные для определенного шифра. Например, для известной шифровальной машины «Энигма» характерной особенностью является то, что никакой символ открытого текста не может быть зашифрован тем же символом. Тогда можно построить критерий проверки, записав его, например, так:

Если $E(x_i) = x_i$, то доказано, что для зашифрования использована не «Энигма»; здесь x_i – произвольный символ открытого текста, $E(x)$ – функция зашифрования.

Сформулируйте аналогичные критерии проверки того, был ли для зашифрования применен шифр «Два квадрата» с одним (неизвестным) ключом. Для получения максимального балла сформулируйте не менее 5 корректных критериев такой проверки, позволяющих утверждать, что используется указанный шифр или что он не мог быть использован (т. е. использован неопределенный иной шифр). Критерии могут быть описаны в любой форме – например, в виде формальных условий (как в примере выше) в текстовой форме или иначе. (5 баллов)

_____

_____

_____

ИБ 9_____

ЧЕРНОВИК

Внимание: черновик сдается организаторам вместе с бланком ответа на кейс-задание.
Записи черновика при проверке работ не учитываются.

К заданиям №№ 18 – 20:

Таблица кодировки ASCII

Обозначения:

DEC – код символа в десятичной системе счисления,

HEX – код символа в шестнадцатеричной системе счисления,

BIN – код символа в двоичной системе счисления,

Символ – соответствующий кодируемый символ.

DEC	HEX	BIN	Символ	DEC	HEX	BIN	Символ
48	30	00110000	0	87	57	01010111	W
49	31	00110001	1	88	58	01011000	X
50	32	00110010	2	89	59	01011001	Y
51	33	00110011	3	90	5A	01011010	Z
52	34	00110100	4	97	61	01100001	a
53	35	00110101	5	98	62	01100010	b
54	36	00110110	6	99	63	01100011	c
55	37	00110111	7	100	64	01100100	d
56	38	00111000	8	101	65	01100101	e
57	39	00111001	9	102	66	01100110	f
65	41	01000001	A	103	67	01100111	g
66	42	01000010	B	104	68	01101000	h
67	43	01000011	C	105	69	01101001	i
68	44	01000100	D	106	6A	01101010	j
69	45	01000101	E	107	6B	01101011	k
70	46	01000110	F	108	6C	01101100	l
71	47	01000111	G	109	6D	01101101	m
72	48	01001000	H	110	6E	01101110	n
73	49	01001001	I	111	6F	01101111	o

DEC	HEX	BIN	Символ	DEC	HEX	BIN	Символ
74	4A	01001010	J	112	70	01110000	p
75	4B	01001011	K	113	71	01110001	q
76	4C	01001100	L	114	72	01110010	r
77	4D	01001101	M	115	73	01110011	s
78	4E	01001110	N	116	74	01110100	t
79	4F	01001111	O	117	75	01110101	u
80	50	01010000	P	118	76	01110110	v
81	51	01010001	Q	119	77	01110111	w
82	52	01010010	R	120	78	01111000	x
83	53	01010011	S	121	79	01111001	y
84	54	01010100	T	122	7A	01111010	z
85	55	01010101	U				
86	56	01010110	V				

4ac2629b3926

4ac80cfe723860217cef7373