

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТРУДУ (ТЕХНОЛОГИИ)
ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП
ТЕОРЕТИЧЕСКИЙ ТУР
11 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 сдадите 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. (0,5 балла) На рисунке (А) представлена лазерная трубка лазерно-гравировального станка. Лазерная трубка внешне представляет собой колбу из стекла, которая в свою очередь также состоит из нескольких внутренних стеклянных полостей. Всего лазерная трубка имеет 3 стеклянных контура. Газовая смесь располагается только в центральной колбе, которая также называется газоразрядная трубка (рисунок Б). Контур стекла вокруг газоразрядной трубки предназначен для протока охлаждающей жидкости. В газовой смеси используется три вида газов, каждый из которых отвечает за решение определенной задачи. Какой газ отвечает за выделение энергии в виде фотонов?



Рисунок А. Лазерная трубка.

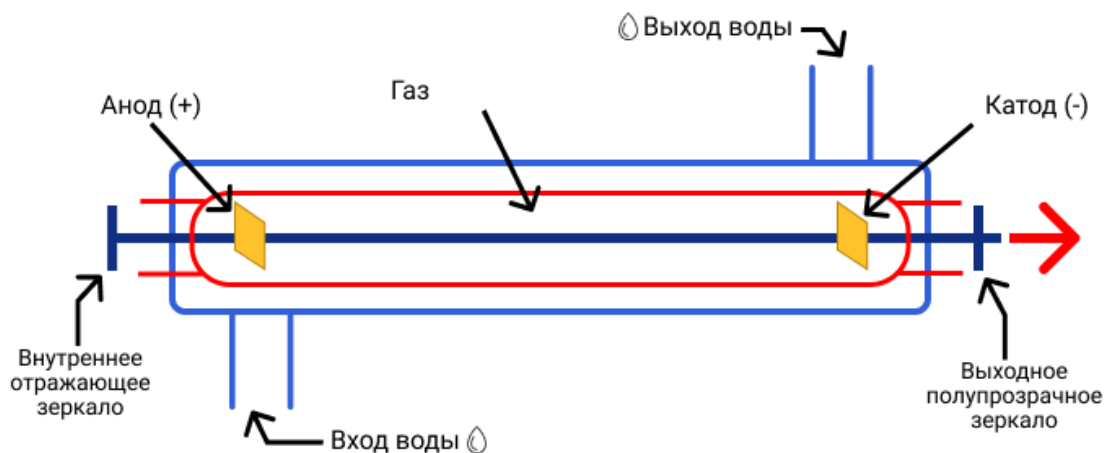
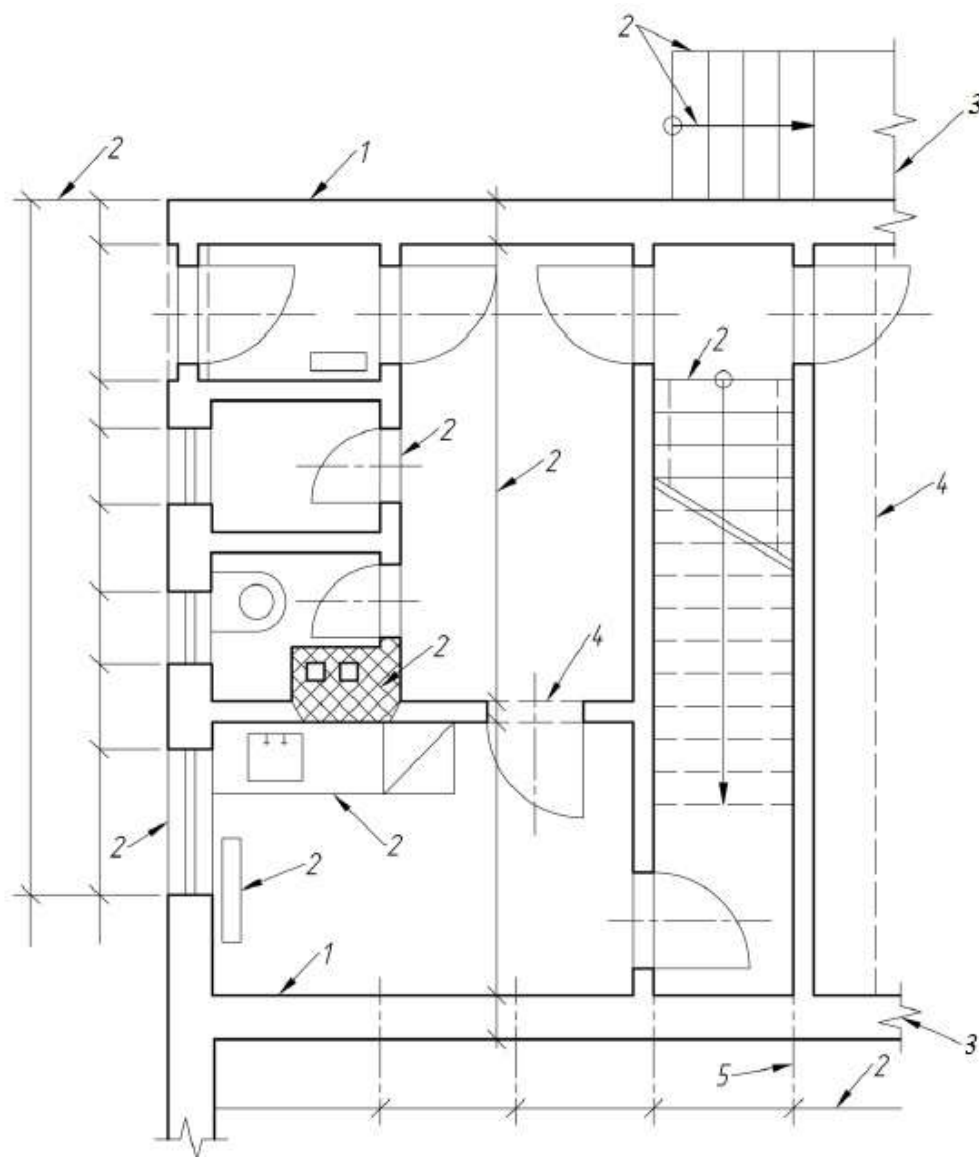
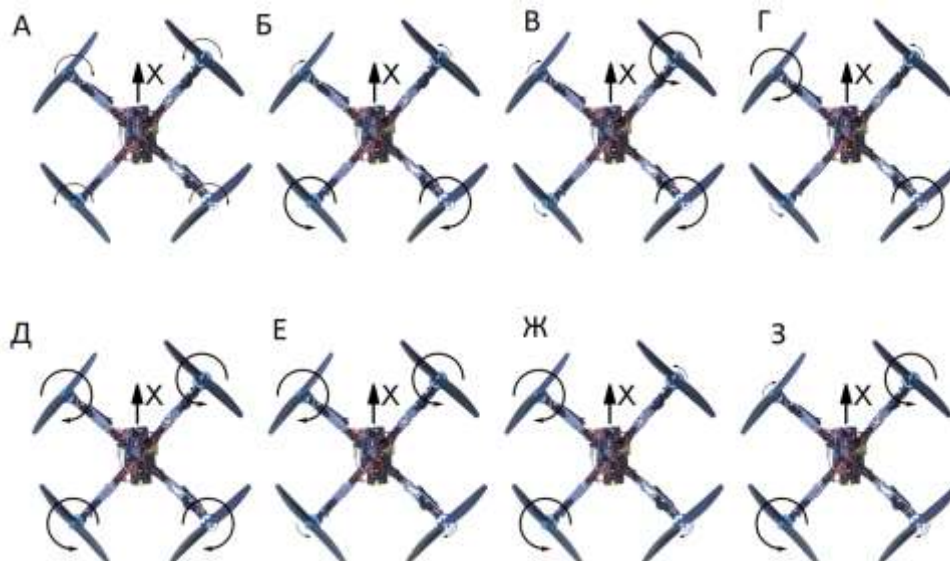


Рисунок Б. Схема устройства лазерной трубки.

2. (1 балл) Ответьте на вопросы: Что изображено на рисунке? Укажите названия линий, представленных на чертеже. В чём основное назначение линии номер 5?



3. (0,5 балла) Выберите два изображения схемы работы винтов, при которых квадрокоптер будет осуществлять набор высоты и выполнять движение назад.



4. (1,5 балла) Для улучшения свойств металлов их соединяют в сплавы. Установите соответствие между компонентами сплава, названием сплава и его применением. Ответ запишите в виде сочетания цифр и букв, например: 1Аа2Бб3Вв4Гг

Компоненты сплава	
1	алюминий, кремний
2	железо и углерод
3	медь и олово
4	медь и никель
5	медь, никель, марганец
6	медь и цинк

	Сплав
А	бронза
Б	константан
В	мельхиор
Г	латунь
Д	сталь
Е	силумин

	Применение сплава
а	изготовления инструментов, шестерёнок и пружин
б	изготовление монет, инструментов, столовых приборов
в	литьё деталей в авто- и моторостроении
г	изготовление электроизмерительных приборов
д	изготовление деталей машин и запорной аппаратуры
е	изготовление проводов с повышенной механической прочностью, пружины и контактные детали для электрических аппаратов и приборов, автомобильные детали, подвижные узлы

5. (0,5 балла) На атомной электростанции в процессе выработки электроэнергии происходят преобразования одних видов энергии в другие. Расположите в правильной последовательности процесс преобразования различных видов энергии при работе АЭС.

- 1 – внутренняя энергия водяного пара
- 2 – внутренняя энергия теплоносителя
- 3 – кинетическая энергия паровой турбины
- 4 – электрическая энергия, вырабатываемая генератором
- 5 – энергия распада атомных ядер в реакторе

6. (1 балл) Компания реализует товар собственного производства по цене 600 руб. за единицу. Постоянные (фиксированные) расходы компании составляют 200 000 руб. Переменные расходы равны 200 руб. за единицу. Определите:

А. – точку безубыточности (самоокупаемости).

Б. – сколько компания должна реализовать дополнительно, чтобы получить прибыль 400 000 руб.

Налоги не учитывайте. Ответ запишите целыми числами.

7. (1 балл) В таблице приведены пиктограммы условных обозначений деталей и узлов механизмов и электрических компонентов согласно «ГОСТ 2.770—68

ЕСКД. Обозначения условные графические в схемах. Элементы кинематики», «ГОСТ 2.703-2011 ЕСКД. Правила выполнения кинематических схем» и «ГОСТ 2-702-2011 ЕСКД. Правила выполнения электрических схем». Определите какая из пиктограмм относится к электротехническим компонентам, а какая к элементам кинематики и распределите их на 2 группы.

1		5		9	
2		6		10	
3		7		11	
4		8		12	

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 без пробелов, например, 3456.

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

8) При выключенных двигателях НПА находится в устойчивом равновесии.

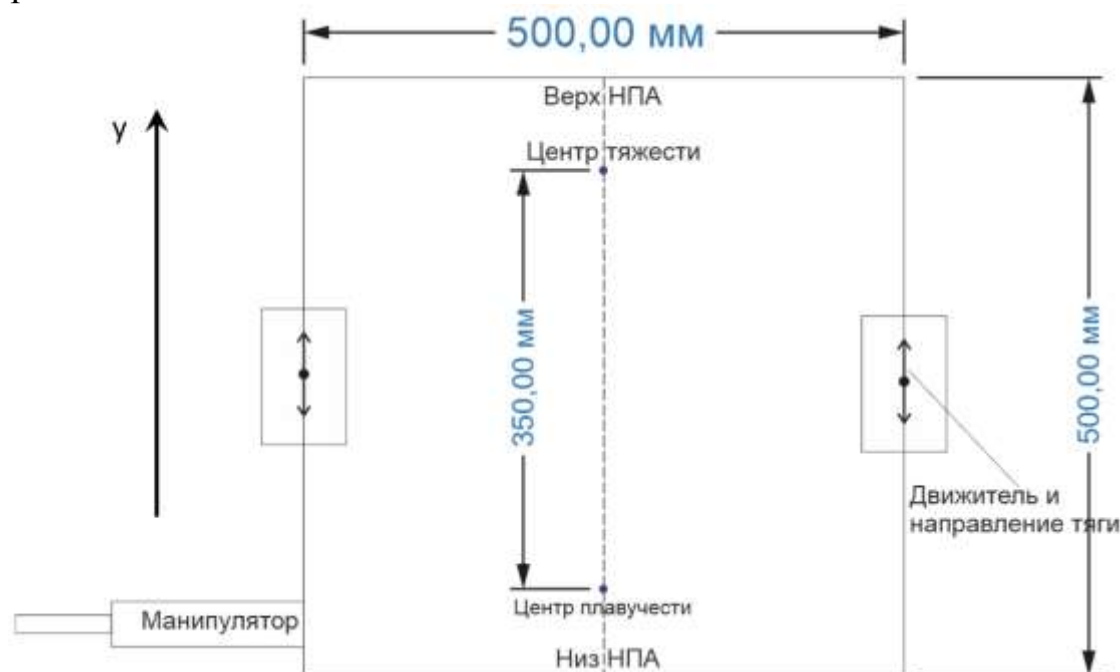


Рис. 1. Необитаемый подводный аппарат

Масса НПА - 11 кг.

Двигатель. Тяга в прямом направлении (совпадает с направлением оси y): 0,3 кгс (при номинальном напряжении). Тяга при реверсе: 0,2 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 блочном шифре, разработанном и используемом в компании “SuperIT”, шифрование происходит следующим образом:

Для шифрования пользователь вводит ключ, длиной 4 бита. Входной блок открытого текста длиной 8 бит делится на 2 подблока равной длины («левый» и «правый»). Далее в каждом раунде происходят следующие операции, результатом которых является также пара из «левого» и «правого» подблоков:

1) К входному «правому» подблоку применили раундовую функцию, состоящую из 3 последовательных действий:

- Сложение по модулю 2 с заданным изначально ключом
- Инверсия
- Циклический сдвиг влево на 1 разряд

Полученный результат сложили с «левым» подблоком по модулю 2. Полученный подблок является результирующим «правым» подблоком.

2) Результирующим «левым» подблоком является «правый» подблок в своем неизменном на момент начала раунда виде (то есть до применения к нему раундовой функции) в следующем раунде.

В ходе шифрования реализуется 3 раунда преобразований.

Результатом шифрования является 8-битовый блок, состоящий из полученных после третьего раунда сначала «правого», а затем «левого» подблоков.

Рассмотрим процесс зашифрования блока «11001001».

9. Определите, сколько существует различных ключей шифрования, при использовании которых на выходе мог быть получен блок «01010101». (2 балла)

10. Приведите все такие ключи в лексикографическом порядке (то есть в порядке возрастания десятичного представления двоичной строки). (2 балла)

Алексей готовился к олимпиаде по информационной безопасности днями и ночами и совсем потерял мотивацию. Вернуть рабочее состояние не удалось, даже восстановив режим. В момент наибольшего отчаяния он получил от своего наставника следующую карточку с мини-заданием:

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

Кажется, ему передали что-то очень важное. Ответьте на следующие вопросы, чтобы помочь Алексею справиться с его проблемой.

11. Определите число символов в скрытом сообщении. (1 балл)
12. Определите число слов в скрытом сообщении. (1 балл)
13. Восстановите скрытое сообщение. (2 балла)

В компании MegaIT произошло заражение вредоносной программой одного из рабочих мест. Системный администратор при помощи антивирусной программы обнаружил ее и установил ее версию при попытке распространения на другие узлы локальной сети. После этого администратором в сети Интернет был найден фрагмент алгоритма работы вредоносной программы в виде блок-схемы:



(схема будет предоставлена отдельным файлом)

Ему также известна структура файлов и папок на зараженном устройстве до заражения:

.

```

└─ C:/
  └─ Users/
    └─ Admin/
      └─ Documents/
        └─ report.docx
        └─ budget.xlsx
      └─ Game/
        └─ PvsZ2/
          └─ Galaxy64.dll
          └─ GalaxyCSharpGlue/
            └─ lib_burst_generated.dll
            └─ Resources/
              └─ ScriptingAssembliesres.json
              └─ sharedassets22.json
              └─ sharedassets0.assets22.resS
              └─ StreamingAssets/
            └─ PBG/
              └─ RuntimeInitializeOnLoadn/
                └─ ScriptingAssemblies.json
                └─ sharedassetsO.assets
                └─ sharedassets0.assets.resS
                └─ sharedassetsO.resource

```



```

| | | | | └─ proj/
| | | | | └─ sem/
| | | | | └─ try/
| | | | | └─ web/
| | | | | └─ web2/
| | | | | └─ aHrn.docs
| | | | | └─ acqu.docs
| | | └─ Downloads/
| | | └─ installer.exe
| | | └─ movie.mp4
| | | └─ Summer/
| | | └─ hedvh.mp4
| | | └─ 01.mp4
| | | └─ rhcvbedvuo687.png
| | | └─ rh01.mp4
| | | └─ jhcjevhibejhce.mp4
| | | └─ r1.jpg
| | └─ Public/
| | └─ SharedDocs/
| | └─ Music/
| | | └─ pl1.mp3
| | | └─ playlist2022.mp3
| | └─ Videos/
| | └─ 01.mp4
| └─ Program Files/
| └─ SoftwareX/

```

```

| | └─ Common Files/
| └─ Windows/
|   └─ bootstat.dat
|   └─ WindowsUpdate.log
|   └─ setupactlog/
|     └─ PFR0.log
|     └─ notepad/
|       └─ rtxplorer.exe
|       └─ DtcInstall.log
|       └─ bfsvc.exe
|       └─ twain_32/
|         └─ MEMORYDMP/
|           └─ HelpPane.exe
|       └─ regedit.exe
|       └─ splwow64.exe
|       └─ System32/
|         └─ WPDShextAutoplay.exe
|         └─ WPDShServiceObj.dll
|         └─ HostNetSvc.dll
|         └─ corever/
|           └─ csup.txt
|           └─ WMSysPr/
|             └─ systemini/
|               └─ mnani/
|                 └─ Core/
|                   └─ CoreSingleLanguage.xml

```

```

|      | |      └─ winhlp32.exe
|      | └─ hh.exe
|      └─ nvspinfo.exe
|      └─ vmcompute.exe
|      └─ vmwp/
|      | └─ provisioningcommandscsp.dll
|      | └─ provlaunch/
|      |   └─ provmigrate.dll
|      |   └─ provplatformdesktop.dll
|      |     └─ FrameServer/
|      |       └─ FrameServerClient.dll
|      └─ Temp/
└─ :D/
|   └─ Plugins/
|   |   └─ SoftwareUpdate.Resources
|   |   └─ SoftwareUpdateFiles.Resources
|   |   └─ ScriptingObjectModel.dll
|   |   └─ SoftwareUpdate.exe
|   |   └─ SoftwareUpdateAdmin.dll
|   |     └─ SoftwareUpdateFiles.dll
|   └─ Bonjour/
|       └─ BonjourResources/
|       └─ dns_sd.jar
|       └─ mdnsNSP.dll
|       └─ mDNSResponder.exe
|       └─ OBonjour/

```

```

|   └─ payment.odt
└─ :E/
    ├── Adobe Animate 2024/
    ├── Dorfromantik_1.1.5.1/
    ├── Inscryption_1/
    |   ├── OST_FLAC.zip
    |   ├── OST_MP3.zip
    |   └─ usetup_inscryption_1.IO_win_(56780).exe
    └─ t.bin
        ├── Keep Talking and Nobody Explodes [Windows]/
        ├── PyCharm 2022.2/
        |   └─ skeletons/
        |       └─ build.txt
        └─ @ product-info.json
            ├── Hosan nanKa/
            ├── Adobe Animate 2024 24.0.0.305 RePack by KpoJluK.exe
            └─ Adobe InDesign 2022 17.0.1.105 RePack by KpoJluK.exe11.

```

14. Установите путь к файлу с копией вредоносной программы, созданному в системе во время заражения. (1 балл)

15. Установите путь к файлу, созданному вредоносной программой, содержащему обнаруженные программой пароли. (1,5 балла)

16. Установите путь к файлу, созданному вредоносной программой, содержащему обнаруженные программой данные банковских карт. (1,5 балла)

Кодирование – это отображение $\varphi: I \rightarrow B$ 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.

Двоичный блочный (n, k) -код преобразует двоичные последовательности длины k (информационные слова) в двоичные последовательности длины n (кодированные слова).

Пример: $(7,3)$ -код: информационное слово – 110 (3 бита), кодовое слово – 0111110 (7 бит).

Подобное преобразование позволяет обнаруживать и исправлять ошибки (искажения битов), которые происходят при передаче кодовых слов по каналу связи.

Расстоянием Хэмминга $d(x, y)$ 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 Хэмминга с искаженным.

Пример:

Искаженное кодовое слово 001.

Множество кодовых слов: {000, 111}.

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

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) удастся 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.

Циклический код – блочный код, у которого все циклические сдвиги кодового слова так же являются его кодовыми словами.

Циклические коды задаются с помощью генераторного многочлена $g(x)$, который является делителем многочлена $x^n - 1$, где n — длина кода. Кодовые слова представляются в виде многочленов, и каждое кодовое слово делится на $g(x)$ без остатка.

Рассмотрим циклический код с длиной кода $n = 7$ и генераторным многочленом $g(x) = x^3 + x + 1$. Этот код может обнаруживать и исправлять одиночные ошибки.

Информационное сообщение $m(x)$ имеет длину $k = 4$.

Чтобы закодировать $m(x)$, нужно выполнить следующие шаги:

1. Умножьте $m(x)$ на x^{n-k}
 2. Разделите результат на $g(x)$ и найдите остаток $r(x)$.
 3. Кодовое слово $c(x)$ получается как $m(x) * x^{n-k} + r(x)$.
17. Закодируйте информационное сообщение $m(x) = x^3 + x^2 + x + 1$ (что соответствует битовой последовательности 1111) с использованием генераторного многочлена $g(x) = x^3 + x + 1$. В ответе укажите сообщение в виде битовой последовательности. (2 балла)
18. Пусть принято сообщение $c'(x) = x^6 + x^5 + x^3 + x + 1$. Известно, что в сообщении присутствует единичная ошибка. Исправьте сообщение и укажите его в ответе в виде битовой последовательности. (3 балла)

19. Кейс-задание

Ученик 10 класса Петя узнал об алгоритме хэширования на основе российского ГОСТ «Стрибог» и предложил идею, как ускорить его работу в 2 раза. Для этого он предложил вычислять значение функции не от всей последовательности исходных данных, а лишь от ее нечетных байтов, считая справа налево (в случае, если последовательность оканчивается неполным нечетным байтом, он

дополняется до полного байта чередующейся последовательностью нулей и единиц (0, 010, 0101 и т. д.).

Оцените, обладает ли получившаяся функция хэширования качествами, требуемыми от криптографической функции хэширования, проанализировав ее на основе требований к таким функциям. Для получения максимального балла рассмотрите не менее 5 параметров качества функции хэширования. *(5 баллов)*