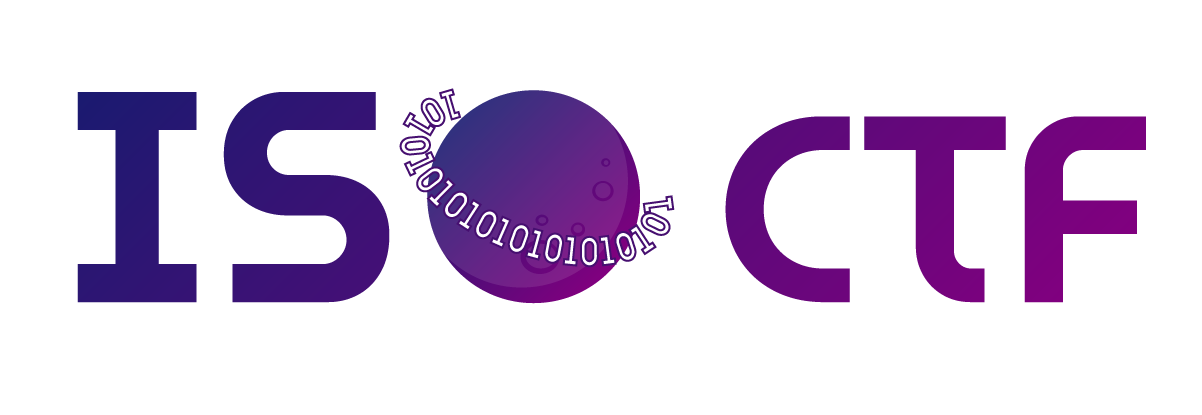
**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДСКОГО ОКРУГА КОРОЛЁВ МОСКОВСКОЙ ОБЛАСТИ «ЛИЦЕЙ №5»**

Пионерская ул., 34, г.о Королёв Московской области

тел +7 498 748-42-33

**Использование игрового формата с космической тематикой для подростков в виде перехвата флага онлайн ISO.CTF**

**Авторы работы: Мирошниченко Анастасия Романовна**

**ученица 10 «А»**

**Северина Дарья Константиновна**

**ученица 11 «А»**

**Научный руководитель:**

**Корбут Татьяна Николаевна, учитель информатики и математики**

**Королев 2020**

**Содержание:**

[**1. CTF**](#_auguxull6fl) **4**

[**1.1 Что такое CTF**](#_1hzqapbbgfo3) **4**

[**1.2 Стеганография**](#_4yqmbnte7urr) **4**

[**1.3 Криптография**](#_ynof81avqkhi) **7**

[**1.4 OSINT**](#_ysjdhndwgkg7) **8**

[**1.5 PPC (Professional Programming and Coding)**](#_r6go6y2zjgv) **9**

[**2. Разработка площадки и заданий.**](#_i5l2jy8dmac3) **10**

[**2.1 Почему мы выбрали Jeopardy**](#_f0galyqqbw1) **10**

[**2.2 Разработка заданий**](#_u3j8xwikste8) **10**

[**2.3 Разработка сайта**](#_tmtnyzqtay0g) **11**

[**2. 4 Условия задач с их решениями**](#_xbnczk5j1lso) **11**

[**Источники информации:**](#_7ku2w453cej6) **14**

**Введение**

Мы раздумывали каким наилучшим образом вызвать интерес школьников-подростков к двум важнейшим в наше время темам — космос и IT. И самым удачным решением проблемы стал выбор формата CTF. Таким образом можно будет предоставить информацию в интересной игровой форме. Также ее реализация вполне нам по силам.

**Актуальность:**

Наш проект будет актуален, ведь в наше время многие подростки интересуются подобными вещами, и ISO.CTF станет хорошей помощью начать.

**Цель работы**: С помощью игровой формы привлечь молодежь к проблеме информационной безопасности и приобщить к космосу. Мы раздумывали каким наилучшим образом вызвать интерес школьников к двум важнейшим в наше время темам — космос и IT. И самым удачным решением проблемы стал выбор формата CTF.

**Задачи:**

1.Проанализировать источники информации по заявленной теме.

2. Разработать задачи, необходимых для проведения соревнования.

3. Разработать сайт, для выполнения контеста.

4. Синхронизировать задачи и сайт.

**Гипотеза:** Предполагается, что проведения данного контеста, включающий в себя задания разных категорий и интересной информации о космосе, привлечет внимание школьников к двум важным сферам: IT и космос.  
  
**Методы работы:**

1. Анализ источников информации.
2. Моделирование.
3. Анализ и обобщение полученных данных

**1. CTF**

### **1.1 Что такое CTF**

CTF (Capture The Flag) — это индивидуальные или командные соревнования по информационной безопасности.

Задания могут относиться к одной из следующих категорий: CTF делится на jeopardy и attack/defence. Различие в том, что в jeopardy игроками или командами решаются задачи нескольких категорий, о которых мы расскажем позже. В attack/defence игроки или команды атакуют удаленные машины друг друга по защищенному каналу, который заранее предоставят организаторы соревнования.

### **1.2 Стеганография**

Стеганография — способ передачи или хранения [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F) с учетом сохранения в тайне самого факта такой передачи (хранения). Этот термин ввёл в [1499 году](https://ru.wikipedia.org/wiki/1499_%D0%B3%D0%BE%D0%B4) [аббат](https://ru.wikipedia.org/wiki/%D0%90%D0%B1%D0%B1%D0%B0%D1%82) бенедиктинского монастыря Св. Мартина в Шпонгейме [Иоганн Тритемий](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B8%D1%82%D0%B5%D0%BC%D0%B8%D0%B9,_%D0%98%D0%BE%D0%B3%D0%B0%D0%BD%D0%BD) в своём трактате «Стеганография» ([лат.](https://ru.wikipedia.org/wiki/%D0%9B%D0%B0%D1%82%D0%B8%D0%BD%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Steganographia*), зашифрованном под магическую книгу.

В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок, письмо или судоку. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

В конце 1990-х годов выделилось несколько направлений стеганографии:

* классическая,
* компьютерная,
* цифровая.

**Классическая стеганография**

### Одним из наиболее распространенных методов классической стеганографии является использование симпатических (невидимых) чернил. Текст, записанный такими чернилами, проявляется только при определенных условиях (нагрев, освещение, химический проявитель и т. д.).Изобретенные еще в I веке н. э. Филоном Александрийским, они продолжали использоваться как в средневековье, так и в новейшее время, например, в письмах русских революционеров из тюрем. В советское время школьники на уроках литературы изучали рассказ, как Владимир Ленин писал молоком на бумаге между строк. Строки, написанные молоком, становились видимыми при нагреве над пламенем свечи.

**Компьютерная стеганография**

Компьютерная стеганография - это направление классической стеганографии, основанное на особенностях компьютерной платформы. Примеры — стеганографическая файловая система StegFS для Linux, скрытие данных в неиспользуемых областях форматов файлов, подмена символов в названиях файлов, текстовая стеганография и т. д. Приведем некоторые примеры

* Использование зарезервированных полей компьютерных форматов файлов — суть метода состоит в том, что часть поля расширений, не заполненная информацией о расширении, по умолчанию заполняется нулями. Соответственно мы можем использовать эту «нулевую» часть для записи своих данных. Недостатком этого метода является низкая степень скрытности и малый объем передаваемой информации.
* Метод скрытия информации в неиспользуемых местах гибких дисков — при использовании этого метода информация записывается в неиспользуемые части диска, к примеру, на нулевую дорожку. Недостатки: маленькая производительность, передача небольших по объёму сообщений.
* Метод использования особых свойств полей форматов, которые не отображаются на экране — этот метод основан на специальных «невидимых» полях для получения сносок, указателей. К примеру, написание черным шрифтом на чёрном фоне. Недостатки: маленькая производительность, небольшой объем передаваемой информации.

**Цифровая стеганография**

Цифровая стеганография — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Но, как правило, данные объекты являются мультимедиа-объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов. Кроме того, в оцифрованных объектах, изначально имеющих аналоговую природу, всегда присутствует шум квантования; далее, при воспроизведении этих объектов появляется дополнительный аналоговый шум и нелинейные искажения аппаратуры, все это способствует большей незаметности сокрытой информации.

### **1.3 Криптография**

Криптография — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), шифрования (кодировка данных).

Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел [симметричных криптосистем](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D1%8B%D0%B5_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B), в которых шифрование и расшифрование проводится с использованием одного и того же секретного ключа.

Пример: шифр Цезаря, в котором информация зашифровывается при помощи при помощи сдвига.

### **Криптографические примитивы.**

* Симметричное шифрование
* DES, AES, Blowfish, IDEA, RC4
* Асимметричное шифрование

RSA и Elgamal

* Цифровые подписи (ЭЦП)
* Хэширование

MD4, MD5, MD6, SHA-1, SHA-2

### **1.4 OSINT**

Разведка на основе открытых источников (англ. Open source intelligence, OSINT) — разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из общедоступных источников, а также ее анализ. В разведывательном сообществе термин «открытый источник разведывательных данных», который указывает на общедоступность источника (в отличие от секретных источников и источников с ограниченным использованием), но он не связан с понятиями «просто источник информации», означающий любую находящуюся в пространстве СМИ информацию. Это понятие не тождественно «публичной разведке».

Открытые источники для разведки:

* СМИ — газеты, журналы, радио, телевидение.
* Интернет, в частности веб-сообщества и контент, созданный пользователями — социальные сети, видеохостинги, вики-справочники, блоги, веб-форумы.
* Публичные отчеты правительства, официальные данные о бюджетах, демографии, материалы пресс-конференций, различные публичные заявления.
* Наблюдения — радиомониторинг, использование общедоступных данных дистанционного зондирования земли и аэрофотосъемок.
* Профессиональные и академические отчеты, конференции, доклады, статьи.

### **1.5 PPC (Professional Programming and Coding)**

Олимпиадное программирование — интеллектуальное соревнование по решению различных задач на ЭВМ, для решения которых необходимо придумать и применить какой-либо алгоритм или программу на одном из языков программирования. Как правило участникам выдается комплект из нескольких задач. Задача считается решенной, если участники смогли составить программу, которая правильно работает на тестах, подготовленных жюри. Тесты участникам неизвестны.

Олимпиады бывают личные и командные. В командных олимпиадах обычно участвует 3 человека и им на всё время олимпиады предоставляется 1 компьютер для решения задач. Для проведения подобных соревнований используются специализированные программные турнирные системы.

**Задачи**  
 На классических олимпиадах по программированию участникам предлагается некоторый набор задач различного уровня сложности. Решением задачи является программа, написанная на одном из допустимых языков программирования. Эта программа должна корректно считывать любые входные данные указанного формата из определенного входного потока, корректно обрабатывать их согласно условию задачи, и выводить в определенный выходной поток в указанном виде. Для ввода-вывода могут использоваться как стандартные консольные потоки, так и файловые (часто входной файл имеет имя «input.txt», а выходной — «output.txt»).

### **2. Разработка площадки и заданий.**

### **2.1 Почему мы выбрали Jeopardy**

Мы выбрали формат соревнования jeopardy, потому что там много различных категорий, и каждый сможет попробовать себя в роли специалиста по информационной безопасности. Также,у каждого участника есть мотивация победить из-за конкуренции Для jeopardy можно придумать как легкие, так и сложные тематические задачи (в нашем случае о космосе), которые будет интересно решать. С другой стороны командные олимпиады улучшают навыки работы в команде, возможно участники хорошо подружатся, и продолжат улучшать свои навыки вместе

### 2.2 Разработка заданий

Было выбрано 4 категории:

* Stegano
* Crypto
* PPC
* OSINT

Мы выбрали именно эти категории, потому что новичкам, которые видят этот формат впервые, так будет проще понять, что к чему, быстрее влиться в игру. Например, можно взять категории pwn и reverse. Но для них нужно хорошо уметь работать с консолью, не теряться в удаленной машине и иметь высокие навыки программирования. Относительно выбранных нами заданий, все участники будут равны по знаниям.

### **2.3 Разработка сайта**

Для начала мы разработали макет, сделали наброски того, чего хотелось бы видеть. Большую роль сыграло удобство, поэтому для создания сайта мы выбрали площадку “Tilda”. Таким образом, мы облегчили работу и оптимизировали действия. Отчеты того, что вышло в процессе, вы можете увидеть в презентации. Не стоит забывать, что директор нашего “Лицея №5” финансово вложились в разработку сайта.

### 

### **2. 4 Условия задач с их решениями**

Разборы заданий можно будет увидеть на наших страницах в GitHub.  
Дарья Северина - <https://github.com/Nomichannn>  
Анастасия Мирошниченко - <https://github.com/b3ck3rz>

Нашей первой задачей будет задание на криптографию - Aliens from MSR-17.

**Условие:** К нам прилетели пришельцы с планеты MSR-17, и мы их угостили нашими любимыми блюдами: борщом, варенной картошкой, хлебом и салатом “цезарь”. Но им пришел по вкусу только цезарь. Напоследок они оставили нам послание, но мы их не поняли. Не поможешь нам?

**Решение:**

-При решении данной задачи стоило обратить внимание на слова цезарь и 17.

-Найти сервис, который декодирует цезарь очень просто, соответственно мы переводим данный текст при 17 “обороте”.

-А вот и флаг!

Следующей задачей станет задание на стеганографию - Space matryoshka.

**Условие:**

Обычная матрешка, но последняя кукла немного поломалась.

**Решение:**

* Перед нами изображение. Можно попытаться открыть его в блокноте, посмотреть метадату, но правильным решением будет открыть изображение как архив, так как это RarJPEG. Мы получаем 6 файлов, но важны нам всего лишь 3.
* Стоит обратить внимание на файл «hey\_kitten.jpg». На картинке написано, что пароль - это название корабля, на котором Гагарин полетел в космос, также стоит учесть, что пароль в нижнем регистре. Зачем нам это? Картинка также является RarJPEG, а пароль от файлов это «восток-1».
* Мы получаем три файла, обращаем внимание на текстовый файл «broken». Мы находим кусочек флага, но выглядит он немного странно и его нужно привести в порядок. Перед нами один из известнейших эзотерических языков - Brainfuck. Его надо скомпилировать, мы получаем часть флага «m4tr10shk4s!}».
* У нас есть файлы, названия которых - цифры. Это очередность каждой части флага, осталось их найти.
* Файл «1.png» стоит открыть в программе *Stegsolve* и посмотреть цветовые каналы. На одном из них будет часть флага, а именно его начало «iso{w3\_».
* Осталась середина флага, она будет в файле «2.jpg». Смотрим метадату файла, видим в комментариях строку текста - это кодировка ASCII, декодировав ее, мы получаем последнюю часть флага «l0v3\_sp4c3\_}».
* Объединив все части, воедино мы получаем цельный флаг.

Новое задание - Uncommon matryoshka.

**Условие:**

К нам прибыл уникальный экспонат неизвестного происхождения. Наши ученые назвали его космической матрешкой. Попробуем узнать, что она скрывает в себе?

\*показывается файл\*

**Решение:**

* Нам уже дана подсказка в самом задании, большая часть завязана на знании языков и терпении
* Очевидно, что это Brainfuck, соответственно мы будем компилировать его несколько раз, пока не получим флаг

Завершающее задание - Blend S-pace

**Условие:**

Нам кажется, что работник под кодовым именем MENAD отправляет данные третьим лицам. Чтобы узнать это, нужно вторгнуться в его компьютер. Ходят слухи, что его пароль это первые буквы некоторых космонавтов. Формат флага: iso{\*ваш ответ\*}.

**Решение:**

* Решение задания очевидно - Найти в поисковике по фотографиям имена космонавтов, предложенных в архиве.

### **Источники информации:**

[https://ru.wikipedia.org/wiki/Олимпиады\_по\_программированию](https://ru.wikipedia.org/wiki/%D0%9E%D0%BB%D0%B8%D0%BC%D0%BF%D0%B8%D0%B0%D0%B4%D1%8B_%D0%BF%D0%BE_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8E)

<https://ctftime.org/>

[http://itsecwiki.org/index.php/Заглавная\_страница](http://itsecwiki.org/index.php/%D0%97%D0%B0%D0%B3%D0%BB%D0%B0%D0%B2%D0%BD%D0%B0%D1%8F_%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D0%B0)

<https://habr.com/ru/post/64216/>

https://kmb.cybber.ru/