CTF шаг в цифровое будущее

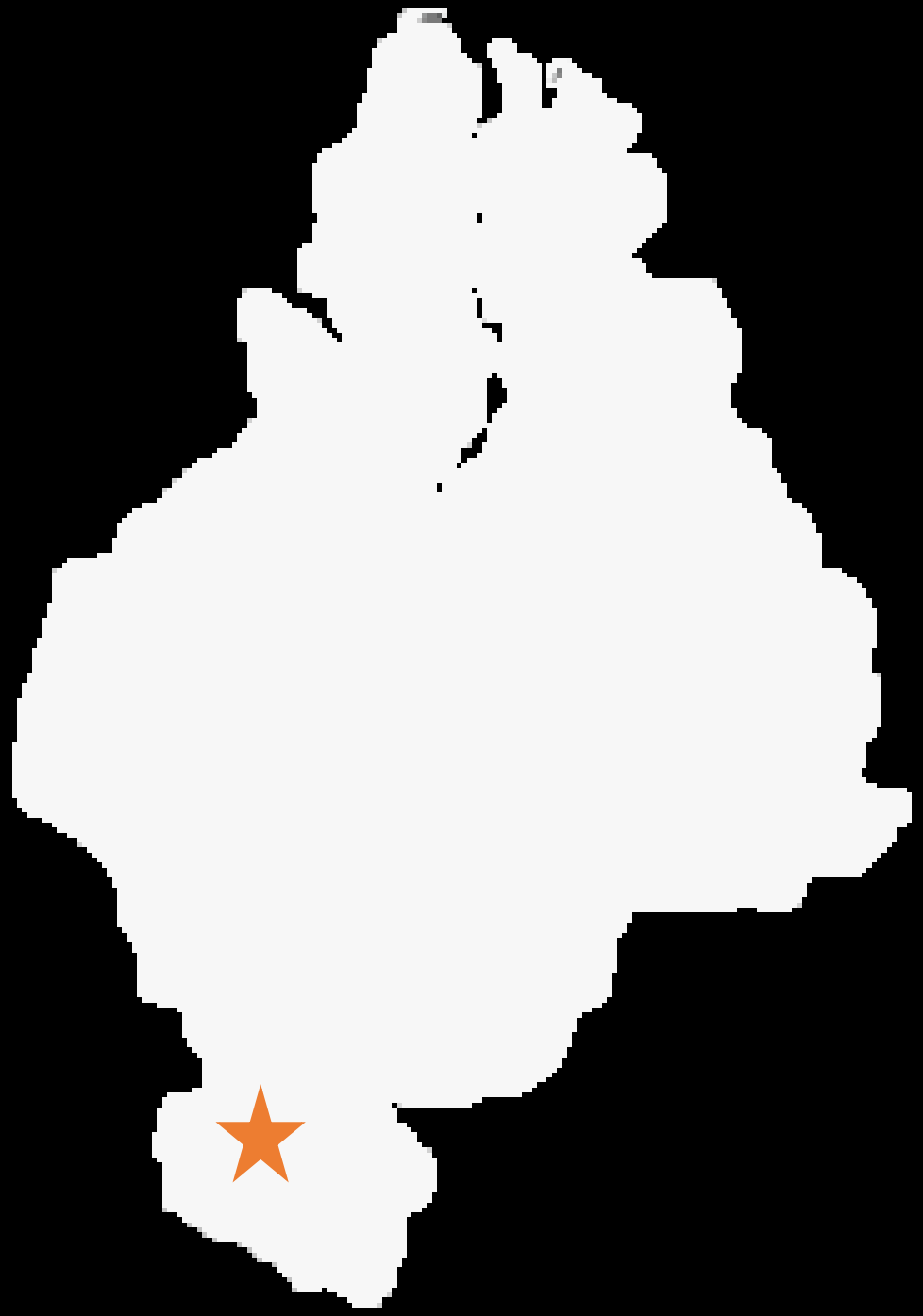
Зулькарнеев Искандер Рашитович
доцент кафедры информационной безопасности ИМиКН ТюмГУ
Координатор CTF-соревнований по УрФО
тел. 8-919-959-4040, e-mail: i.r.zulkarneev@utmn.ru

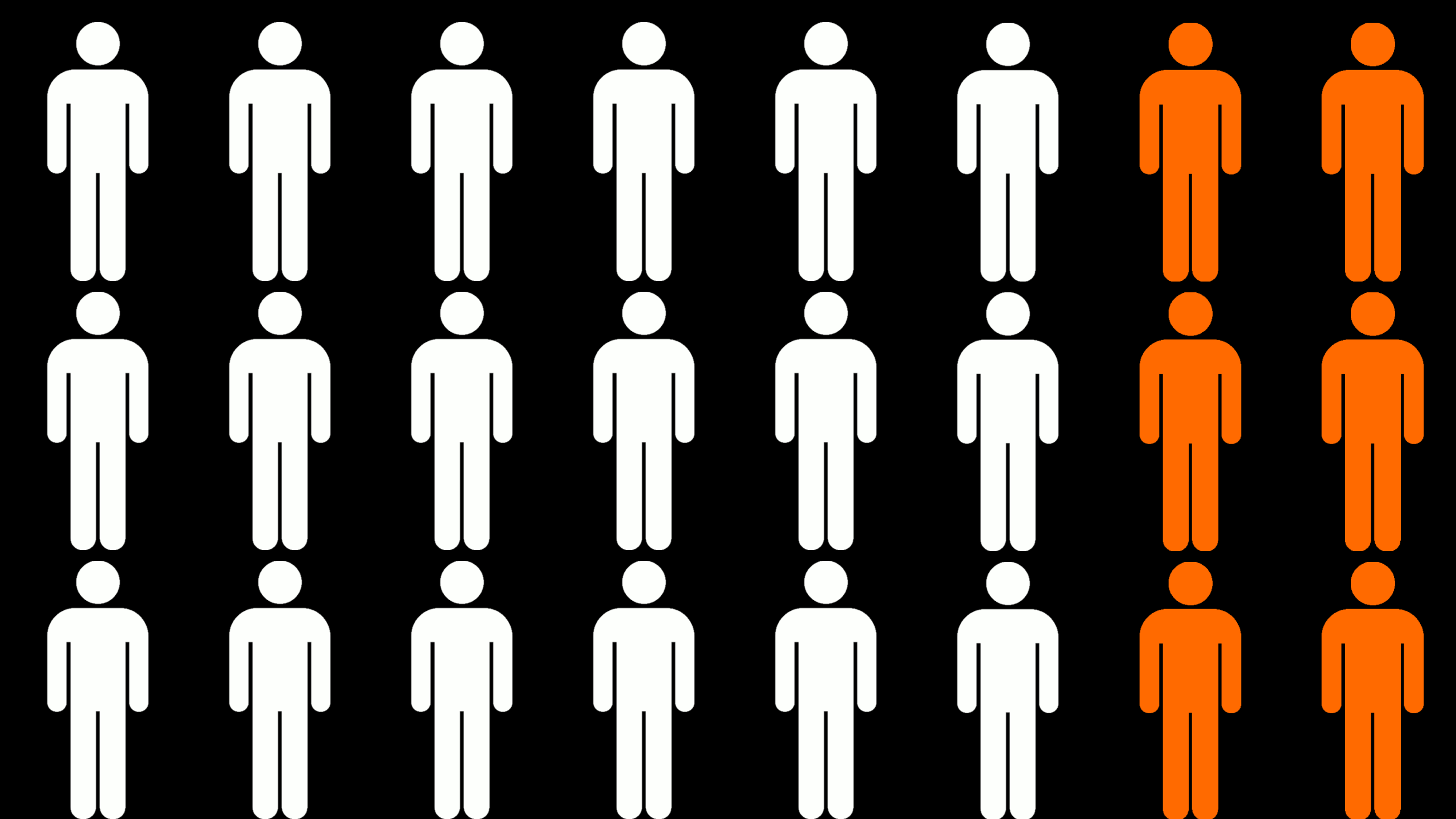
Информационная безопасность

и

ТюмГУ

- ✓ Приоритетное направление
- ✓ Востребованность на рынке труда
- ✓ Единственные в Тюменской области, ХМАО и ЯНАО
- ✓ Набор в 2019г.: 160 человек





Компьютерная безопасность

специалитет, 5 лет 6 месяцев

- ✓ Проектирование систем защиты информации
- ✓ Управление информационной безопасностью
- ✓ Отражение компьютерных атак
- ✓ Компьютерная криминалистика
- ✓ Более глубокая фундаментальная подготовка

Информационная безопасность автоматизированных систем

специалитет, 5 лет

- ✓ Техническая защита информации
- ✓ Защита распределенных систем
- ✓ Защита локальных сетей и веб-ресурсов
- ✓ Более глубокая техническая подготовка

Информационная безопасность

бакалавриат, 4 года

- ✓ Базовые навыки и знания по информационной безопасности
- ✓ Равномерная подготовка по всем дисциплинам
- ✓ Возможность выбрать специализацию в магистратуре
- ✓ Возможность работы по инженерным профессиям в области ИБ

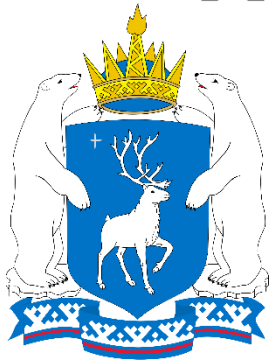
POSITIVE TECHNOLOGIES

KASPERSKY lab

GROUP IB

INFOWATCH®

ТюмГУ



infotecs®

КОД БЕЗОПАСНОСТИ

Ежегодные онлайн соревнования **TyumenCTF** и спортивные соревнования **Киберзарница**

Открытые лекции с ведущими российскими экспертами в области информационной безопасности

Межрегиональные открытые соревнования по информационной безопасности **UralCTF**

Призеры всероссийских соревнований
Победители межрегиональных соревнований
Призеры всероссийских олимпиад
Победители всероссийских конференций

Capture the Flag

Что такое CTF?

Capture the Flag («Захвати флаг») – командные соревнования, в которой проверяются знания и умения участников в сфере информатики, информационных технологий и защиты информации

Цель: поиск и захват секретной информации («флага»): специального файла, кодовой фразы или набора символов.

Пример формата флага
UralCTF{…},
TyumenCTF{…}

TyumenCTF{it_was_cool}

TyumenCTF{3a4gko34l;l$l;v4}

TyumenCTF{r}

Task-based (jeopardy) CTF

- до 7 человек в команде
- задания разного уровня сложности поделены по категориям
- 6-8 часов (если очно)
- можно пользоваться Интернетом
- можно пользоваться своим ноутбуком и программами
- при равенстве очков побеждает первый набравший

Криптография	Форензика	Веб	PPC
100	100	100	100
200	200	200	200
300	300	300	300
400	400	400	400

Категории заданий

Форензика, reverse	• Расследование инцидентов, исследование программ
Стеганография	• Поиск спрятанной, сокрытой информации
PPC	• Классическое программирование
Веб	• Анализ веб-приложений, поиск веб-уязвимостей
Крипто	• Задачи связанные с шифрованием данных
Osint	• Поиск информации из открытых источников
Joy	• Задачи развлекательного характера
Admin	• Задачи на администрирование систем и сетей

Зачем CTF?

Почему CTF и информационная безопасность?

- Постоянное быстрое развитие технологий
- Единое информационное пространство
- Вовлеченность ИТ во все сферы нашей жизни
- Рост числа киберпреступлений
- Политика государства в области обеспечения кибербезопасности
- Популяризация современных идей и технологий
- Потребность в квалифицированных кадрах

Чем полезен CTF?

- Понимание современных технологий
- Развитие логического, аналитического и системного мышления
- Поиск нетривиальных подходов к решению проблем
- Повышения качества и количества знаний и навыков в информатике и программировании

Чем полезен CTF?

- Воспитание культуры и этичного подхода к поиску и эксплуатации уязвимостей («белому хакингу»)
- Привитие ответственности за свои действия
- Совершенствование навыков поиска полезной информации
- Развитие навыков командной работы

Зачем это нужно школьнику?

Подготовка к сдаче ЕГЭ по информатике

- Знание о системах счисления и двоичном представлении информации в памяти компьютера
- Знание о файловой системе организации данных или о технологии хранения, поиска и сортировки информации в базах данных
- Умение кодировать и декодировать информацию
- Знание основных конструкций языка программирования, понятия переменной, оператора присваивания
- Умение осуществлять поиск информации в сети Интернет
- Умение создавать собственные программы
- Умение анализировать программу, использующую процедуры и функции
- Знание основных понятий и законов математической логики
- Умение исполнить рекурсивный алгоритм
- Умение прочесть фрагмент программы на языке программирования и исправить допущенные ошибки

Зачем это нужно школьнику?

2 Поступление в ВУЗы без экзаменов

Олимпиада НТИ

Олимпиада Национальной технологической инициативы по профилю «Информационная безопасность

Межрегиональная олимпиада школьников им. И. Я. Верченко по профилю «Компьютерная безопасность»

RuCTF 2019

Всероссийские соревнования по информационной безопасности с международным участием

Зачем это нужно школьнику?

3 Преимущества при поступлении в ТюмГУ

www.bonus-utmn.ru

Бонусная карта ТюмГУ

- Получение баллов за участие в мероприятии
- Получение баллов за призовые места в мероприятии
- Каждые 1000 баллов = +1 балл при поступлении в ТюмГУ
- Обмен баллов на полезные вещи и сувенирную продукцию

Зачем это нужно школьнику?

4 Стажировка в ведущих компаниях и школах в области информационной безопасности и ИТ

Ростелеком

POSITIVE TECHNOLOGIES

KASPERSKY lab

Сириус
Образовательный центр

GROUP IB

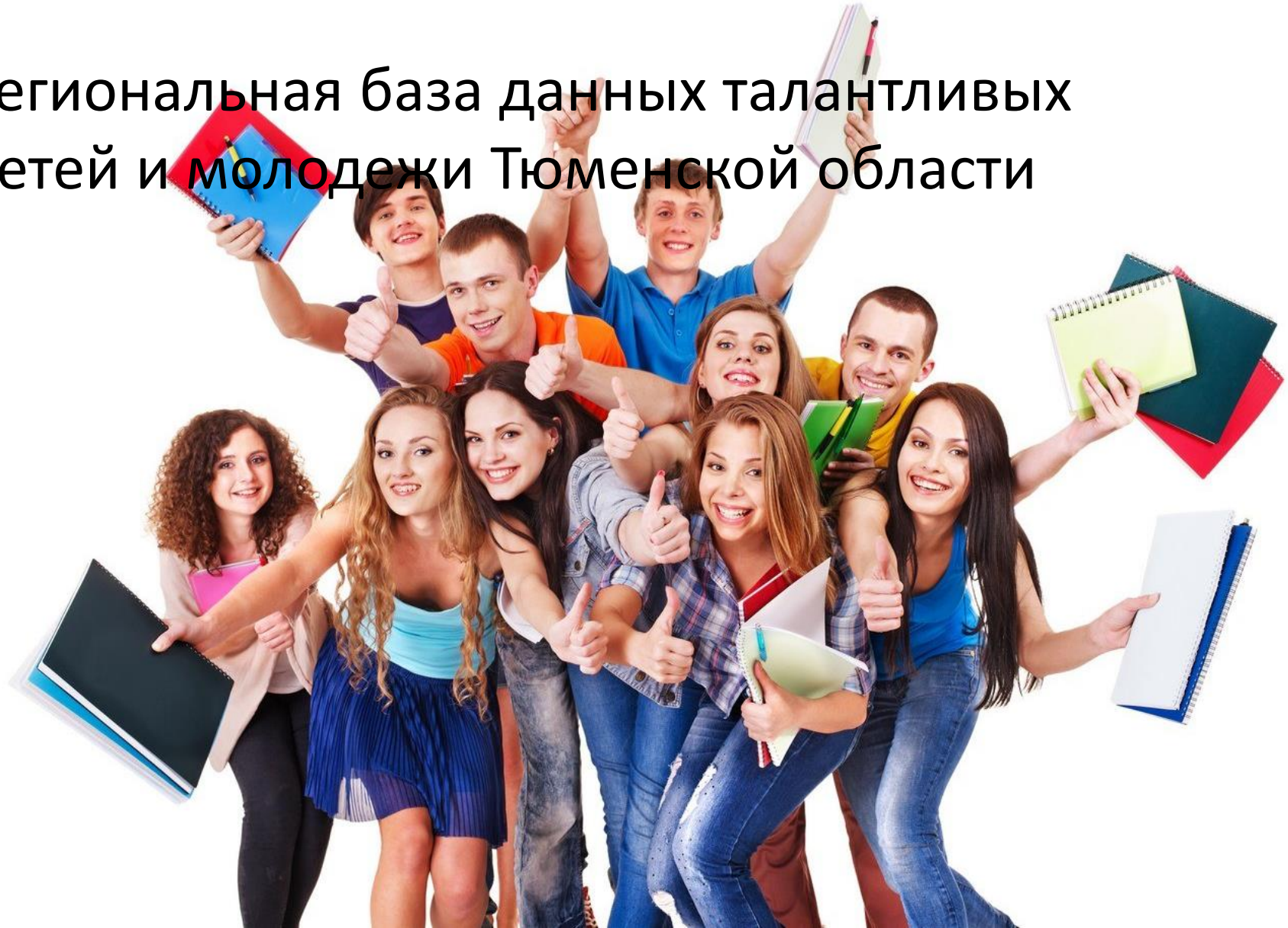
Анлим-ИТ
защищая вашу информацию

Зачем это нужно школьнику?

5 Поступление в Академии ФСБ, Минобороны, ФСТЭК

Зачем это нужно школьнику?

6 Региональная база данных талантливых детей и молодежи Тюменской области



Зачем это нужно учителям?

1. Повышение квалификации в области ИТ
2. Поощрения за успешные выступления школьников
3. Благодарности учителям-тренерам от Департамента образования Тюменской области
4. Ваши предложения …

CTF в нашем регионе

CTF в России

Построение пятиуровневой системы

- Локальных школьные и вузовские, региональные, межрегиональные, всероссийские, международные соревнований

География распространения

- Все крупные города России, все Федеральные округа и специализированные соревнования по отраслям

Поддержка государственных структур

- Минобразования, Минобороны, Минкомсвязи, Академия ФСБ Росси, ФСТЭК России
- Администрация Президента
- Полпред Президента в УрФО
- Губернатор Тюменской области

Академия кибербезопасности

Академия кибер безопасности

Февраль

Киберзарница

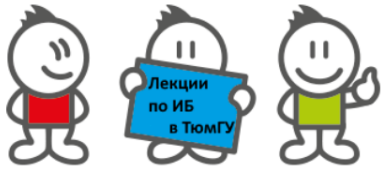
Киберзарница в Тюменском Технопарке в рамках Всероссийского месяца информационной безопасности, и на открытом воздухе в летнее время

Март

TyumenCTF 2019

Международные онлайн соревнования по информационной безопасности для начинающих школьников и студентов TyumenCTF 2019

Июнь



Открытые лекции

Открытые лекции для школьников и студентов младших курсов по углубленному изучению информационной безопасности и подготовке к соревнованиям

Июль

Relationship

Летняя школа ТюмГУ

Летняя инженерно-техническая школа ТюмГУ для школьников 8-10 классов

Октябрь

UralCTF 2019

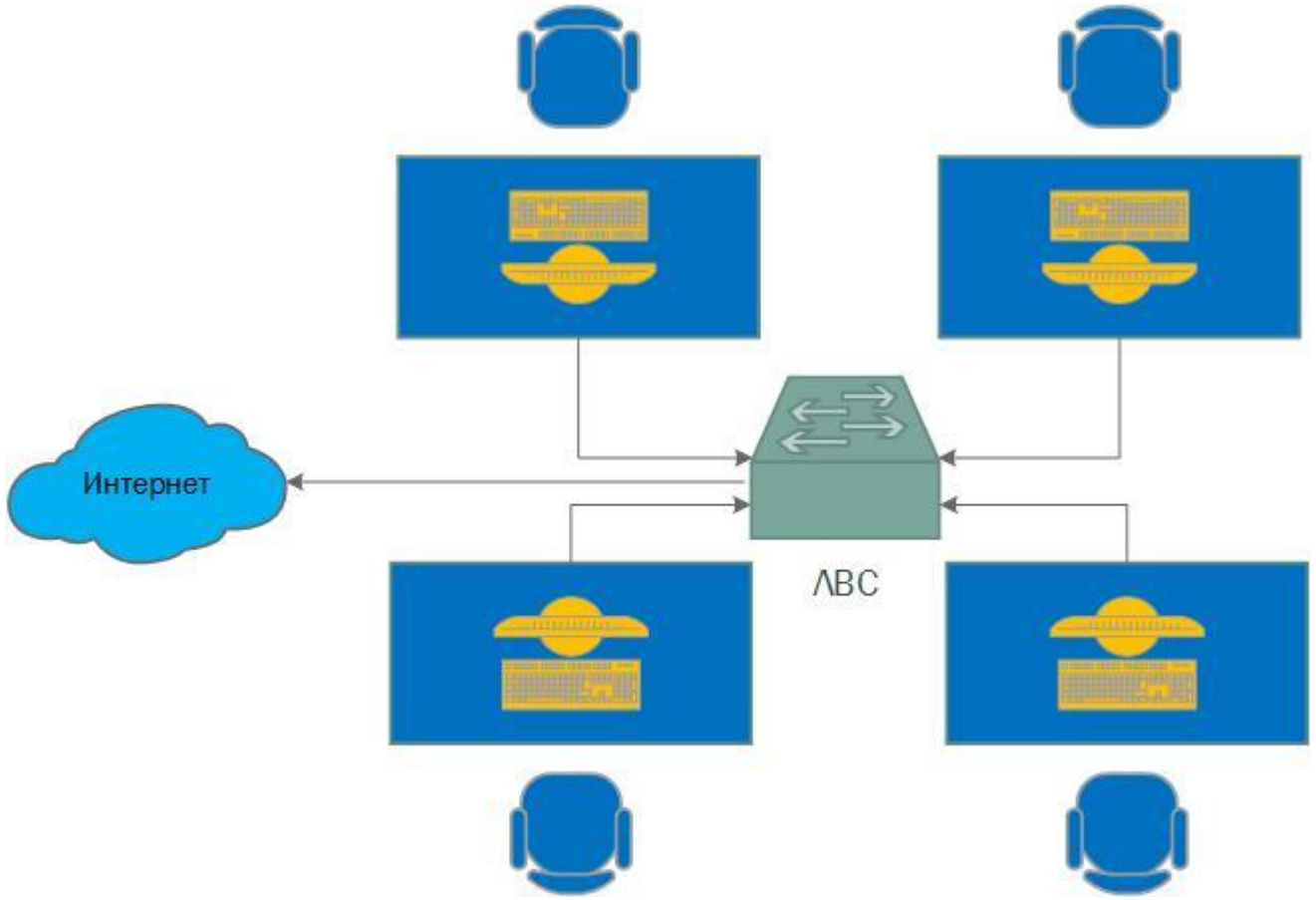
Всероссийские открытые соревнования по информационной безопасности для школьников и студентов UralCTF 2019

Ноябрь

Участие в соревнованиях

Участие в сторонних соревнованиях по информационной безопасности, в том числе в финальном этапе - "Кубок CTF России"

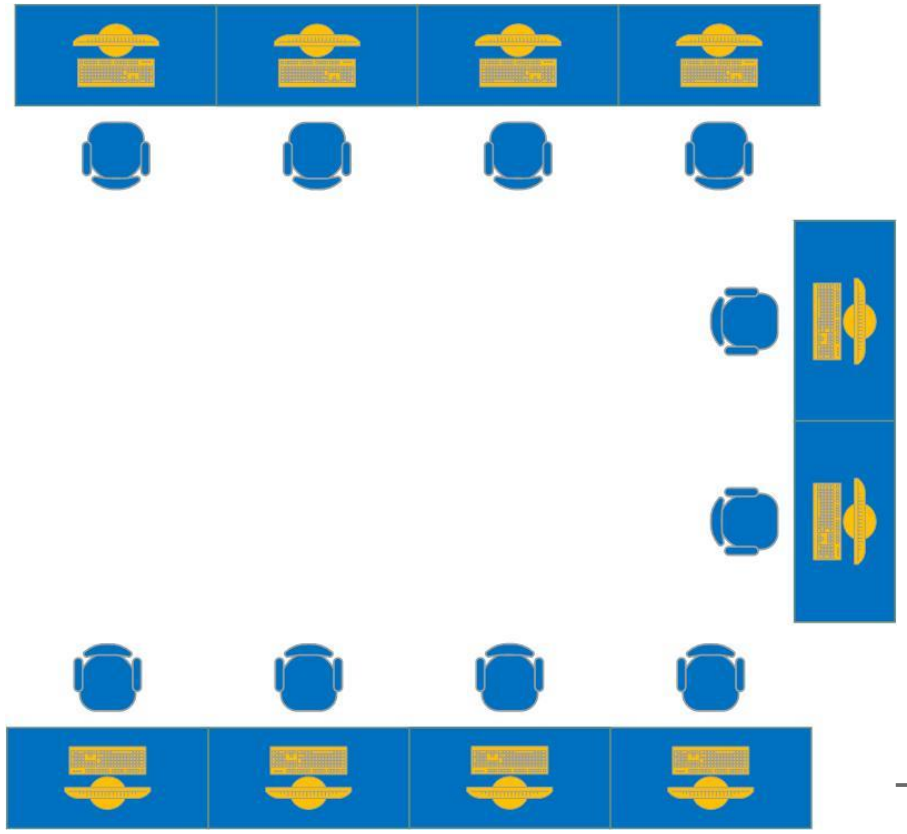
Что нужно для участия в CTF?

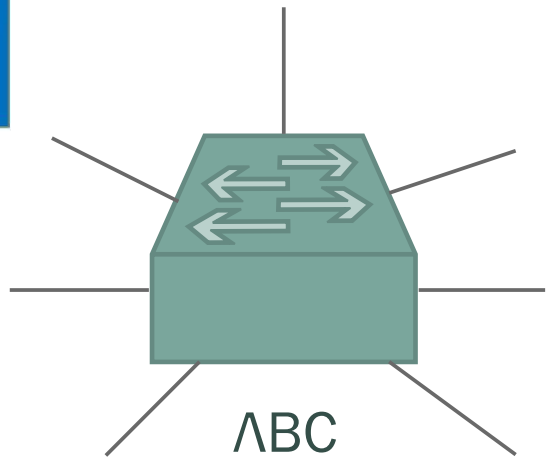


- ✓ Помещение
- ✓ Компьютерные мощности
- ✓ Локальная вычислительная сеть
- ✓ Доступ в Интернет
- ✓ Программное обеспечение
- ✓ Команды учеников
- ✓ Учитель, куратор, занятия, клубы, кружки

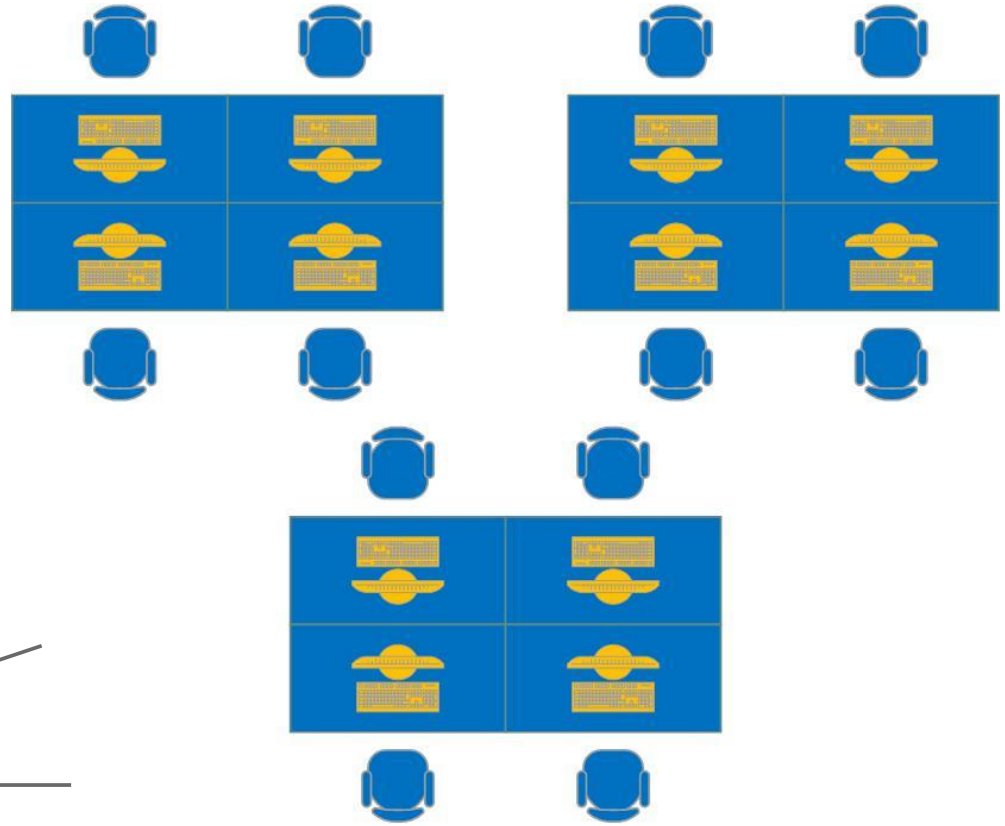
Помещение и сеть

Компьютерные классы





Актовые залы



Компьютеры и программное обеспечение

Стационарный ПК

Ноутбук

Личный ноутбук

Необходимо **свободно распространяемое** программное обеспечение:

- ✓ Браузеры
- ✓ ПО для программирования (C#, Python, Java и т.д.)
- ✓ Просмотр изображений, видео, аудио
- ✓ Сканеры и анализаторы сети
- ✓ Kali Linux
- ✓ Дополнительные специализированные программы

Мы готовы Вам помочь!

- ✓ Обучение и методическая помощь учителям (очно и онлайн)
- ✓ Проведение лекций и семинаров для школьников (очно и онлайн)
- ✓ Подготовка необходимого набора программного обеспечения
- ✓ Создание единого онлайн-платформы, как базы знаний и площадки для тренировок
- ✓ Помощь и проведение локальных соревнований

Примеры заданий

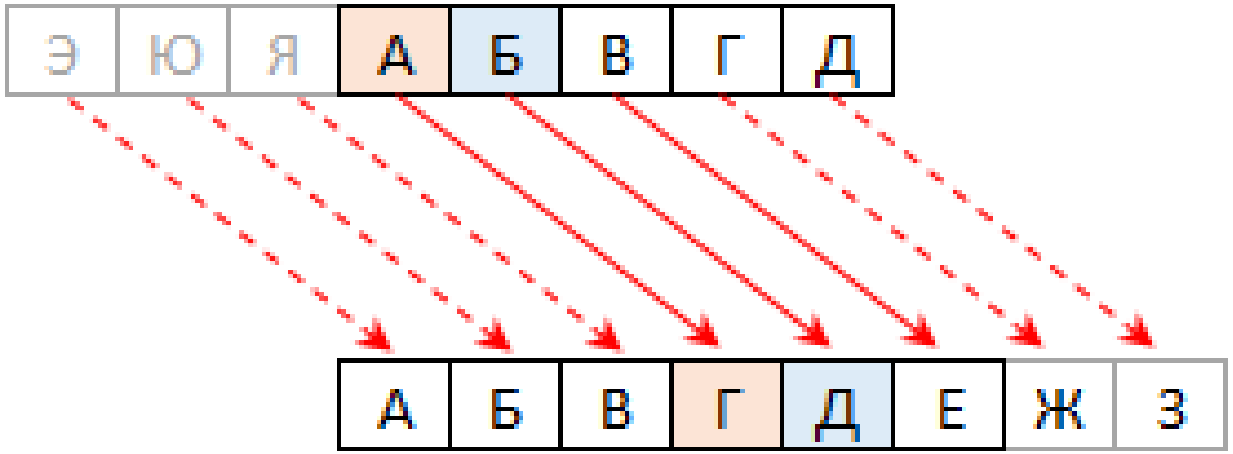
Криптография (шифрование)

Привет! Мой друг, Цезарь, с которым мы дружим уже три года, прислал мне сообщение, но я не могу понять, что оно значит. Может быть ты поможешь мне?

«В ОБДОБ НУЛТХСЁУГЧЛБ!»

Криптография (шифрование)

Шифр Цезаря – замена символов со сдвигом по алфавиту. Каждый символ открытого текста заменяется символом, находящимся правее на величину сдвига



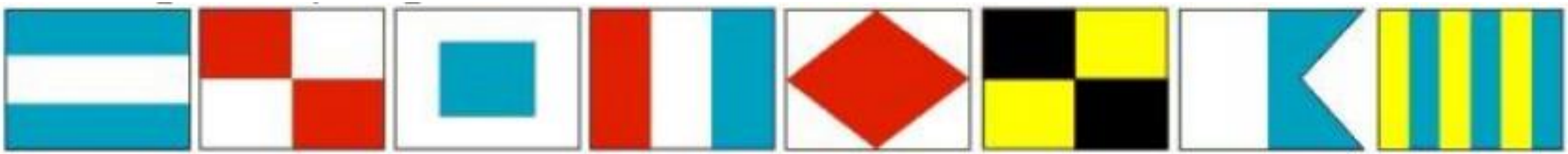
Криптография (шифрование)

Таблица для сдвига, равного 3

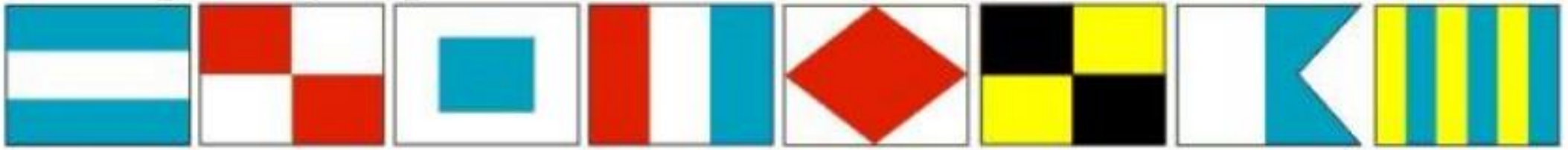
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В

«Я люблю криптографию!»

Стеганография

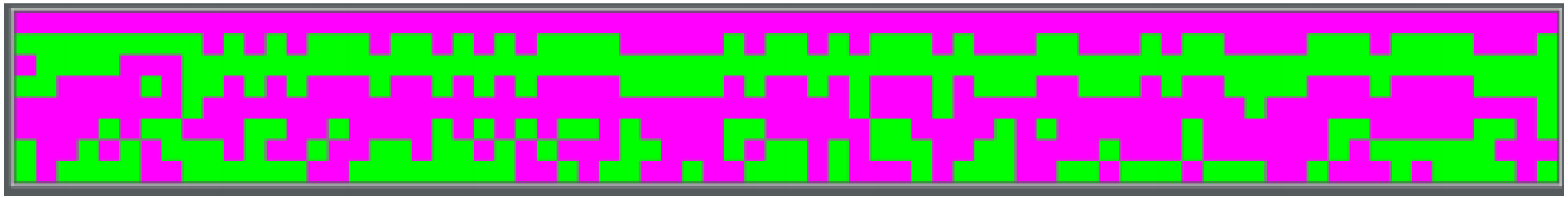


Стеганография

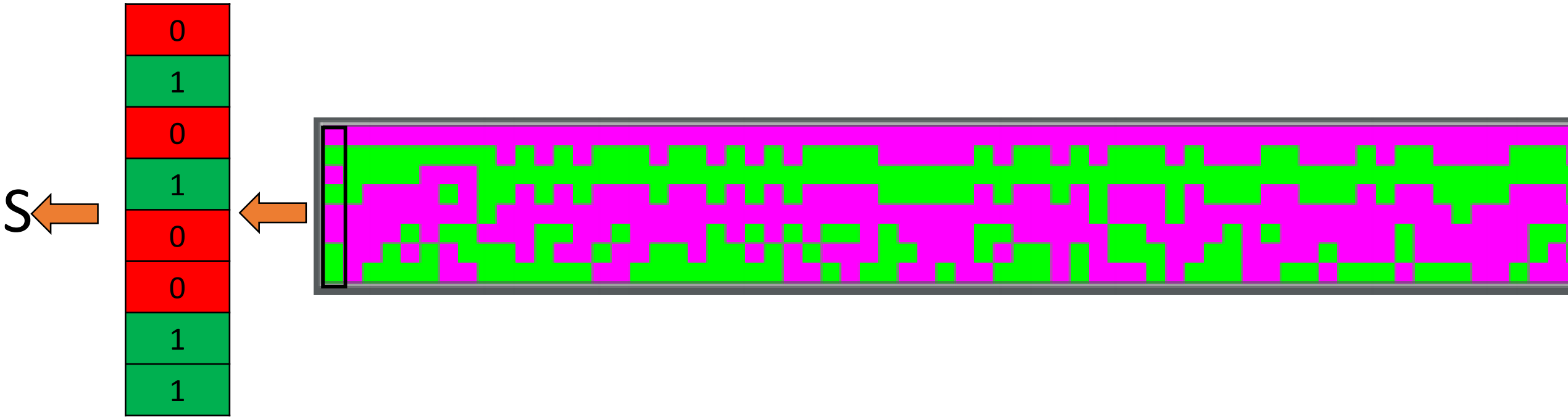


JUSTFLAG

Стеганография



Стеганография



Стеганография

```
from PIL import Image
img = Image.open('bits.png')
img_pixels= img.convert("RGB")
bits=[]
width,height=img.size
for i in range(0,width):
  for j in range(0,height):
     r,g,b=img_pixels.getpixel((i,j))
     if(r==255):
       bits.append('0')
     if(r==0):
       bits.append('1')
message = ''.join(bits)
print(message)
```

Полезные ссылки

https://vk.com/ctf_tyumgu - группа ВК CTF-движения ТюмГУ

https://www.youtube.com/user/h4ckerdom - видеоканал Хакердома

http://training.hackerdom.ru/ - сборник заданий Хакердома

https://ctfnews.ru/ - главный интернет-ресурс CTF-движения в России

http://kmb.ufoctf.ru/ - база знаний CTF от команды UFO

https://goo.gl/eWzEo4 - подборка инструментов, помогающих в решении CTF

itsecwiki.org/index.php?title=Заглавная_страница – подборка примеров заданий по категорий с решениями

Спасибо за внимание!

Зулькарнеев Искандер Рашитович
доцент кафедры информационной безопасности ИМиКН ТюмГУ
Координатор CTF-соревнований по УрФО
тел. 8-919-959-4040, e-mail: i.r.zulkarneev@utmn.ru