



Возможности использования нейросетей при подготовке к урокам

Анна Олеговна Ершова, заместитель
директора МБОУ «СОШ №68 г. Челябинска»,
учитель информатики

Подборка
сервисов на
основе
нейросетей для
преподавателей
и методистов

0
1

GigaChat,
YandexGPT 3

0
2

Gamma.app

0
3

Perplexity, Yeschat

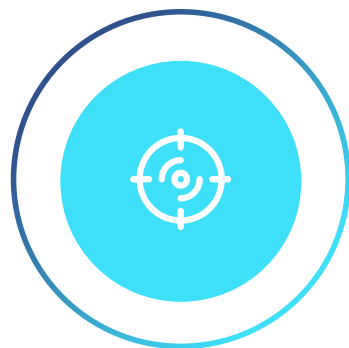
0
4

Kandinsky 3.1





Создавать презентации: нейросеть может создать уникальные изображения по Вашему запросу, которые помогут сделать презентацию более наглядной и интересной для учеников. Или полностью создать презентацию с нуля




Сгенерировать упражнения и примеры: можно использовать нейросеть для создания упражнений по грамматике, диалогов на иностранном языке или объяснений сложных концепций







Решать задачи: нейросеть может прорешать задачи по предметам. Можно попросить учеников проанализировать полученные ответы.



Формировать ассоциации: нейросеть может помочь в запоминании сложных тем, предложив ассоциации, которые облегчат понимание материала для учеников.



















Доступные модели 


Чат **Готовые промпты** Выбор профессии ▾


   

Работа с текстом


GPT-5 (Скоро будет...)

-  Gemini-1.0-Pro 
-  Gemini-1.5-Flash 
-  Sber GigaChat-Pro
-  Sber GigaChat-Lite+
-  YandexGPT-Pro
-  YandexGPT-Lite
-  OpenAI-o1-preview
-  OpenAI-o1-mini
-  GPT-4-Omni 
-  GPT-4o-mini 
-  GPT-4-turbo
-  **GPT-3.5-turbo** 
-  GPT-3.5-turbo


 Новая беседа

Поиск...  **Найти**


Я учитель информатик ... 31 октября 2024


Я учитель информатики у пятого 


Создать схему методо ... 21 октября 2024

Создать схему методологическог 

тест по информационн ... 8 октября 2024

тест по информационной безопас 

 Задайте вопрос

 ?

0.00

4. Программа, наносящая вред компьютеру или пользо

3.

Сопоставьте меру безопасности с ее описанием:

A) Антивирусное программное обеспечение

B) Двухфакторная аутентификация

C) Регулярное обновление программ

D) Резервное копирование данных

1. Подтверждение личности пользователя двумя разл

2. Программа, предотвращающая и обнаруживающая ви

3. Обязательное обновление программ для закрытия

<https://chatru.net>

Я учитель информатики у пятого класса. Помоги мне придумать тестовые задания по теме хранение информации на проверку знаний. Составь пять вопросов с множественным выбором с четырьмя вариантами ответов

Уточняем запрос



ответы на ЭТОТ тест

Какой из этих носителей информации имеет наибольшую емкость?

- A) Дискета
- B) DVD-диск
- C) Blu-ray диск
- D) Кассета

4.

Как называется процесс сохранения информации на носитель?

- A) Перезапись
- B) Копирование
- C) Запись
- D) Стирание

5.

Какой из этих носителей информации не является цифровым?

- A) Виниловая пластинка
- B) SSD-накопитель
- C) SD-карта
- D) CD-диск

Надеюсь, эти вопросы помогут вам в проверке знаний ваших учеников!

Конечно! Вот правильные ответы на предложенные вопросы:

1.

Что такое бит?

Правильный ответ: C) Единица измерения информации

2.

Какой из этих носителей информации является самым старым?

Правильный ответ: C) Граммофонная пластинка

3.

Какой из этих носителей информации имеет наибольшую емкость?

Правильный ответ: C) Blu-ray диск

4.

Как называется процесс сохранения информации на носитель?

Правильный ответ: C) Запись

5.

Какой из этих носителей информации не является цифровым?

Правильный ответ: A) Виниловая пластинка

Задания на сопоставление для школьников по теме информационная безопасность

4.

Сопоставьте вид угрозы с примером:

- A) Спам
- B) Фишинг
- C) Ддос-атака
- D) Вредоносное ПО

1. Массовая отправка нежелательной рекламной информации
2. Поддельное веб-сайт, имитирующий официальный для получения личных данных
3. Атака на сервер с целью перегрузки его работой
4. Программа, наносящая вред компьютеру или пользователям

2.

Сопоставьте вид угрозы с примером:

- A) Спам
- B) Фишинг
- C) Ддос-атака
- D) Вредоносное ПО

1. Массовая отправка нежелательной рекламной информации
2. Поддельное веб-сайт, имитирующий официальный для получения личных данных
3. Атака на сервер с целью перегрузки его работой
4. Программа, наносящая вред компьютеру или пользователям

Помоги решить задачу, ответ дай с подробным решением Прибор автоматической фиксации нарушений правил дорожного движения делает цветные фотографии размером 1024×768 пикселей, используя палитру из 4096 цветов. Снимки сохраняются в памяти камеры, группируются в пакеты по нескольку штук, затем передаются в центр обработки информации со скоростью передачи данных $1\,310\,720$ бит/с. Каково максимально возможное количество снимков в одном пакете, если на передачу одного пакета отводится не более 300 секунд

Решение:

1. Определим общее количество пикселей на одном снимке:

$$1024 \cdot 768 = 786\,432 \text{ пикселя.}$$

2. Найдём необходимый объём памяти для одного снимка, используя глубину цвета и количество пикселей:

- глубина цвета 4096 цветов (или $\log_2(4096) = 12$ бит на пиксель);
- объём памяти $786\,432 \cdot 12 = 9\,437\,184$ бита.

1. Вычислим общий объём данных для передачи одного пакета снимков:

- скорость передачи данных $1\,310\,720$ бит/с;
- время передачи одного пакета ≤ 300 секунд;
- общий объём данных $V_{\text{общ}} = 1\,310\,720 \cdot 300 = 393\,216\,000$ бит.

1. Рассчитаем максимально возможное количество снимков в одном пакете:

- максимально возможное количество снимков N_{max} должно быть таким, чтобы общий объём данных был равен $393\,216\,000$ битам;
- пусть n — искомое число снимков;
- тогда максимально необходимое количество бит для передачи всех снимков в пакете будет равно $9\,437\,184n$, что должно быть равно $393\,216\,000$ бит;
- составим уравнение: $9\,437\,184n = 393\,216\,000$.

1. Решим полученное уравнение относительно n :

$$n = \frac{393\,216\,000}{9\,437\,184} \approx 41.65.$$

2. Округлим результат вниз до ближайшего целого числа, учитывая, что максимально возможное количество снимков должно быть целым:

$$n_{\text{max}} \approx 41.$$

Ответ: максимально возможное количество снимков в одном пакете составляет 41 штуку.

 Скопировать ответ

Чат с YandexGPT 4 Pro RC

Помоги придумать сказку о битах и байтах

В далёкой-далёкой стране, где всё состоит из цифр и кодов, жили-были биты и байты. Они были очень разными, но при этом дружили между собой.

Биты были маленькими и шустрыми, они всегда бегали и прыгали, создавая разные комбинации. А байты были большими и спокойными, они медленно передвигались по стране и следили за порядком.

Однажды в стране появились вирусы, которые хотели уничтожить все данные. Биты и байты решили объединиться, чтобы защитить свою страну. Они создали мощную защиту, которая не давала вирусам проникнуть внутрь.

Вирусы были очень злыми и сильными, но биты и байты не сдавались. Они продолжали создавать новые комбинации и следить за порядком. И вот, наконец, вирусы отступили.

Страна была спасена благодаря дружбе и взаимопомощи битов и байтов. Они поняли, что вместе они могут преодолеть любые трудности. С тех пор биты и байты стали ещё ближе и начали помогать друг другу во всём.

И жили они долго и счастливо в своей стране, создавая новые комбинации и защищая её от любых угроз.

 Скопировать ответ

пусть сказка учит переводить байты в биты

В далёкой-далёкой стране, где всё состоит из цифр и кодов, жили-были биты и байты. Они были очень разными, но при этом дружили между собой.

Биты были маленькими и шустрыми, они всегда бегали и прыгали, создавая разные комбинации. А байты были большими и спокойными, они медленно передвигались по стране и следили за порядком.

Однажды в стране появились вирусы, которые хотели уничтожить все данные. Биты и байты решили объединиться, чтобы защитить свою страну. Они создали мощную защиту, которая не давала вирусам проникнуть внутрь. Но вирусы оказались слишком сильными, и тогда биты с байтами решили использовать всю свою мощь.

И тут встал вопрос: как объединить силы битов и байтов? Ведь у них была разная природа и возможности. Тогда биты предложили перевести байты в биты, чтобы создать единую мощную комбинацию.

Байты сначала не поняли, как это сделать, но потом согласились попробовать. И вот, благодаря дружбе и взаимопомощи, биты объяснили байтам, как перевести их в биты. Это было непросто, но вместе они справились.

Когда байты стали битами, их сила увеличилась в несколько раз. Теперь они могли создавать ещё более мощные комбинации и противостоять вирусам. Вирусы отступили, а страна была спасена.

С тех пор биты и байты стали ещё ближе и начали помогать друг другу во всём. Они поняли, что вместе могут преодолеть любые трудности. И жили они долго и счастливо в своей стране, создавая новые комбинации и защищая её от любых угроз.

А все жители страны узнали, как переводить байты в биты и наоборот, чтобы стать сильнее и увереннее в защите своих данных.

Информационная безопасность

Защита данных в цифровом мире

Важный навык для современных

by Анна Ершова
Last edited 1 minute ago

Share Информационная безопасность

Collaborate Share **Export** Embed Publish to site...

Download a static copy of your gamma to share with others.

- Export to PDF
- Export to PowerPoint**
- Export as PNGs

Gradient headings in your gamma will be exported in single color, since PDF and PowerPoint do not currently support them.

For fonts to display correctly in PowerPoint, you may need the following fonts:

- Inter
- Petrona

Tip: you can control card sizing and backdrops in [page setup](#).

Hide "Made with Gamma" badge **PLUS**

[View analytics](#) **Done**

Задание 1: «Сопоставь угрозы и их последствия»

Цель: помочь ученикам понять, какие последствия могут быть у различных угроз информационной безопасности.

Описание: ученикам предлагается сопоставить различные угрозы информационной безопасности (например, вирусы, фишинг, кража личных данных) с их возможными последствиями (например, потеря данных, финансовые потери, ущерб репутации).

Материалы: список угроз и список последствий.

Инструкция:

1. Разделите учеников на группы.
2. Каждая группа получает список угроз и список последствий.
3. Задача учеников — сопоставить каждую угрозу с её возможными последствиями.
4. После выполнения задания ученики обсуждают свои результаты и объясняют свой выбор.

Задание 2: «Найди отличия»

Цель: научить учеников распознавать признаки фишинговых атак и других угроз информационной безопасности.

Описание: ученикам предлагаются две или более веб-страницы или электронные письма, которые выглядят подозрительно. Ученики должны найти отличия между этими страницами или письмами и определить, какое из них является угрозой.

Материалы: несколько веб-страниц или электронных писем, которые выглядят подозрительно.

Инструкция:

1. Покажите ученикам несколько веб-страниц или электронных писем, которые выглядят подозрительно.

Задание 4: «Кто есть кто?»

Цель: познакомить учеников с различными видами вредоносных программ и объяснить, как они работают.

Описание: ученикам раздаются карточки с описанием различных видов вредоносных программ (например, трояны, черви, шпионские программы). Ученики должны определить, к какому виду относится каждая программа.

Материалы: карточки с описанием различных видов вредоносных программ.

Инструкция:

1. Раздайте ученикам карточки с описанием различных видов вредоносных программ.
2. Попросите учеников определить, к какому виду относится каждая программа.
3. Обсудите с учениками, как работают эти программы и как они могут навредить компьютеру.

Задание 5: «Как это работает?»

Цель: показать ученикам, как работает шифрование данных.

Описание: ученикам показывается видео или презентация о том, как работает шифрование данных. Затем ученики выполняют задание, в котором им нужно расшифровать сообщение, используя ключ шифрования.

Материалы: видео или презентация о шифровании данных, задание на расшифровку сообщения.

Инструкция:

1. Покажите ученикам видео или презентацию о том, как работает шифрование данных.
2. Дайте ученикам задание на расшифровку сообщения, используя ключ шифрования.
3. Обсудите с учениками, как шифрование защищает данные от несанкционированного доступа.

добавь примеры этих заданий с решениями

Задание 1: «Сопоставь угрозы и их последствия»

Цель: помочь ученикам понять, какие последствия могут быть у различных угроз информационной безопасности.

Описание: ученикам предлагается сопоставить различные угрозы информационной безопасности (например, вирусы, фишинг, кража личных данных) с их возможными последствиями (например, потеря данных, финансовые потери, ущерб репутации).

Материалы: список угроз и список последствий.

Инструкция:

1. Разделите учеников на группы.
2. Каждая группа получает список угроз и список последствий.
3. Задача учеников — сопоставить каждую угрозу с её возможными последствиями.
4. После выполнения задания ученики обсуждают свои результаты и объясняют свой выбор.

Пример задания:

Угрозы	Последствия
Кража личных данных	Финансовые потери
Фишинг	Потеря данных
Вредоносные программы	Ущерб репутации
Перехват данных	Финансовые потери и ущерб репутации

Задание 3: «Что такое хорошо и что такое плохо?»

Цель: объяснить ученикам, как безопасно использовать интернет и социальные сети.

Описание: ученики получают список правил безопасного использования интернета и социальных сетей. Они должны определить, какие правила являются хорошими, а какие — плохими.

Материалы: список правил безопасного использования интернета и социальных сетей.

Инструкция:

1. Раздайте ученикам список правил безопасного использования интернета и социальных сетей.
2. Попросите учеников определить, какие правила являются хорошими, а какие — плохими.
3. Обсудите с учениками, почему некоторые правила являются хорошими, а некоторые — плохими.

Пример списка правил:

Правила	Оценка
Никогда не предоставляйте свои личные данные незнакомцам	Хорошо
Используйте сложные пароли и меняйте их регулярно	Хорошо
Посещайте только проверенные сайты	Хорошо
Открывайте подозрительные письма и переходите по ссылкам	Плохо
Загружайте файлы с незнакомых сайтов	Плохо

Решение: ученики должны оценить каждое правило. Они должны объяснить, почему они



You

план конспект урока по информационной безопасности для 9 класса с кейс задачами

2024-10-31 14:14:24



YesChat GPT Teacher

План-конспект урока по информационной безопасности для 9 класса

Тема: Основы информационной безопасности

Цели урока:

1. Ознакомить учащихся с основами информационной безопасности.
2. Развить навыки анализа и решения кейсов по безопасности.

с примерами кейсов

Структура урока:

Получить код

1. Введение (10 минут)

- Обсуждение: Что такое информационная безопасность? Зачем она важна?
- Краткий обзор основных понятий: конфиденциальность, целостность, доступность.

2. Основные угрозы информационной безопасности (15 минут)

- Виды угроз: вирусы, фишинг, социальная инженерия.
- Примеры реальных инцидентов.

3. Кейс 1: Фишинг (15 минут)

- Описание ситуации: учащийся получает email с просьбой ввести личные данные.
- Вопросы для обсуждения:

5. Практическое задание (10 минут)

</> Получить к

- Разделить класс на группы. Каждая группа получает свой кейс для анализа (например, использование публичного Wi-Fi, защита паролей и т.д.).
- Группы представляют свои решения и рекомендации.

6. Заключение (5 минут)

- Подведение итогов: основные выводы урока.
- Обсуждение, как применить полученные знания в повседневной жизни.

Домашнее задание:

Написать короткое эссе на тему "Как я могу защитить свою информацию в интернете".

3. Кейс 1: Фишинг (15 минут)

- **Ситуация:** Учащийся получает электронное письмо от "банка", в котором сказано, что его аккаунт заблокирован, и ему необходимо ввести логин и пароль по указанной ссылке.
- **Вопросы для обсуждения:**
 - Каковы признаки фишинга?
 - Что делать в такой ситуации?
- **Обсуждение:** Выработка рекомендаций по распознаванию и предотвращению фишинга.

4. Кейс 2: Вредоносное ПО (15 минут)

- **Ситуация:** Учащийся устанавливает бесплатную игру и замечает, что компьютер стал медленно работать, появляются рекламные всплывающие окна.

добавить примерные решения кейсов

3. Кейс 1: Фишинг (15 минут)

</> Получить к

- **Ситуация:** Учащийся получает электронное письмо от "банка", в котором сказано, что его аккаунт заблокирован, и ему необходимо ввести логин и пароль по указанной ссылке.
- **Вопросы для обсуждения:**
 - Каковы признаки фишинга?
 - Что делать в такой ситуации?
- **Решения:**
 - Не открывать ссылку и не вводить данные.
 - Проверить адрес отправителя и наличие ошибок в письме.
 - Сообщить о попытке фишинга в техподдержку банка.

Кейс 3: Социальная инженерия (15 минут)

- **Ситуация:** Учащийся получает звонок от "технической поддержки", которая просит предоставить доступ к компьютеру для решения проблемы.
- **Вопросы:**
 - Как распознать попытку манипуляции?
 - Какие меры предосторожности следует соблюдать?
- **Решения:**
 - Не предоставлять никакие данные или доступ к компьютеру.
 - Прекратить разговор и перезвонить в официальную поддержку по номеру с сайта компании.
 - Сообщить о звонке родителям или учителю.

Ершова Анна Олеговна

grishutenko_ania@mail.ru