Урок 2. Персональные данные и безопасность при работе с нейросетями

6 класс · Урок 2 из 18 · 45 минут

Вся программа 6 класса

Урок для 6 класса о нейросетях и персональных данных: ученики уберут лишнее из запроса, проверят источник сообщения и различат цифровой и физический риск.

Нейросети помогают работать с текстом и изображениями, но запрос может содержать лишние персональные данные. Научимся сохранять полезную задачу, убирать сведения о людях, проверять подозрительные сообщения и различать цифровую и физическую безопасность.

Содержание урока

1. Цель урока
2. Ход урока
3. Вход в тему: обрезанный снимок
4. Что нужно задаче, а что раскрывает человека
5. Знакомый голос и независимая проверка
6. Два вида безопасности и первый шаг
7. Итоги урока

01. Цель урока

Научить безопасно обращаться с персональными данными при работе с нейросетями и выбирать действие при цифровом или физическом риске.

К концу урока ученики смогут:

- найти персональные данные, в том числе сочетание косвенных признаков;
- объяснить, почему нейросети не следует передавать лишние сведения о себе и других;
- переписать запрос так, чтобы сохранить задачу и убрать данные о людях;
- проверить подозрительное сообщение через независимый канал;
- различить цифровой и физический риск и назвать безопасный первый шаг.

02. Ход урока

Этап	Мин	Учитель	Ученики
1. Вход в тему: обрезанный снимок	6	Собирает версии, объясняет прямые и косвенные сведения.	Ищут, по каким деталям можно узнать человека.
2. Что нужно задаче, а что раскрывает человека	11	Объясняет передачу данных и разбирает редактуру запроса.	Сохраняют полезные условия и убирают лишние сведения.
3. Знакомый голос и независимая проверка	12	Объясняет подделки, разбирает реальный случай.	Выбирают способ проверки собеседника и порядок действий.
4. Два вида безопасности и первый шаг	11	Различает риски, объясняет действия после ошибки.	Классифицируют последствия и составляют безопасный ответ.
5. Итоги урока	5	Проверяет перенос правил на короткие вопросы.	Дают ответ с причиной, исправляют неполное объяснение.
Итого	45		

03. Этап 1. Вход в тему: обрезанный снимок ≈ 6 минут

ГОВОРИМ УЧЕНИКАМ

Сегодня мы разберём, что можно оставить в запросе к нейросети и что лучше убрать. Полезный ответ часто можно получить без имени, фотографии документа и сведений о том, где человек бывает. Нужно заметить эти сведения до отправки.

Вера хочет, чтобы помощник сделал красивое расписание репетиций. Она обрезала верх снимка с фамилией, но внизу остались её подпись «Вера, 6-Б», название студии и время индивидуального занятия. Можно ли по этим данным связать расписание с конкретным человеком? Что вы проверили бы на всём изображении?

Для учителя

Соберите версии о подписи, классе, студии, времени и фоне. Пока не требуйте юридического определения. Все материалы этого урока разбирают на бумаге или на экране учителя: ученики не вводят настоящие сведения и не регистрируются в сервисах.

ГОВОРИМ УЧЕНИКАМ

Персональные данные — сведения, которые относятся к определённому человеку или помогают его определить. Иногда это имя и фамилия, иногда сочетание: класс, студия, время и подпись. На снимке сведения бывают не только в центре: они могут остаться на полях, в названии файла или в тексте рядом. Обрезка одного имени поэтому ещё не решает задачу.

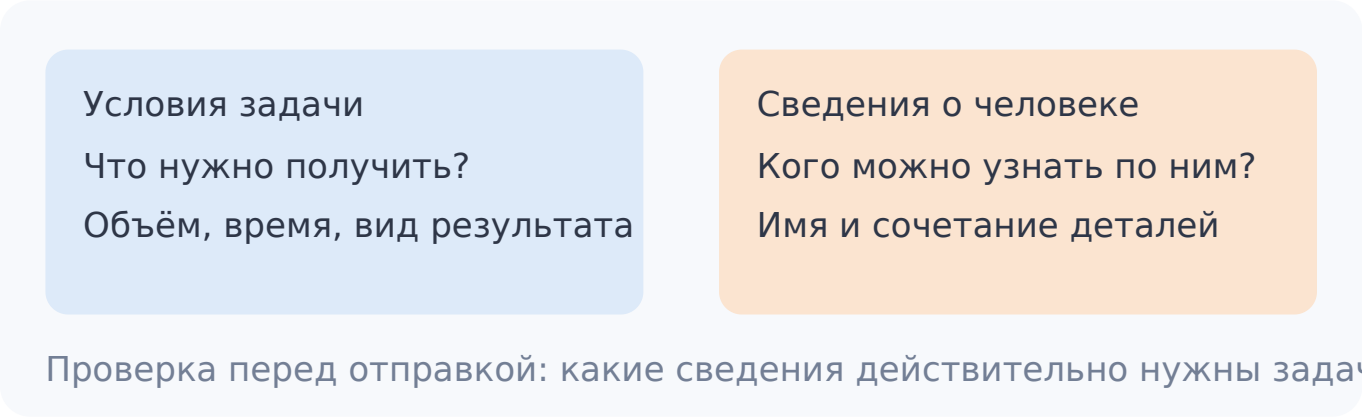
04. Этап 2. Что нужно задаче, а что раскрывает человека

≈ 11 минут

ГОВОРИМ УЧЕНИКАМ

Отправляя запрос, вы передаёте его внешнему сервису для обработки. Как сервис хранит запросы и кто может их видеть, зависит от его устройства и правил. Не следует считать любую переписку с нейросетью личным разговором, который никто больше не сможет увидеть. Утечка — ситуация, когда сведения становятся доступны тем, кому они не предназначались.

Сначала определите, что сервису нужно для задачи. Количество участников и продолжительность встречи помогают составить план. Домашние адреса и фотографии пропусков для такого плана не нужны. Чужие данные требуют такой же осторожности, как свои. Пароли и одноразовые коды защищают доступ к аккаунту: их не включают в запрос вообще.



Полезные условия и сведения о человеке — разные части запроса. Схема автора урока.

Таблица 1. Условия задачи, сведения о человеке и секреты доступа выполняют разные роли.

Роль сведений	Что они позволяют сделать	Что проверить перед отправкой
Сведения о человеке	Узнать человека напрямую или по сочетанию деталей.	Нужна ли такая привязка для результата?
Секрет доступа	Подтвердить вход или действие в аккаунте.	Пароли и коды в запрос не включают.
Условия задачи	Задать вид и объём результата без привязки к человеку.	Достаточно ли этих условий для полезного ответа?

Сохраните задачу, уберите сведения

Артём помогает организовать обмен учебниками после занятий и хочет отправить нейросети таблицу участников, чтобы не переписывать условия вручную. В таблице указаны имена, телефоны для связи и учебники для обмена. Черновик запроса: «Составь план встречи для 24 учеников 6-Б на 30 минут. Раздели участников на четыре группы и предложи порядок обмена. Прикладываю таблицу участников».

1. Выпишите условия, которые нужны для плана.
2. Составьте запрос из двух-трёх предложений без сведений о конкретных людях.
3. Решите, что делать с приложениями. Проверьте, не потерялось ли условие о четырёх группах.

Для учителя: ответы и обсуждение

Нужны 24 участника, 30 минут, обмен учебниками, четыре группы и порядок работы. Приемлемый запрос: «Составь план обмена учебниками для 24 участников на 30 минут. Раздели их на четыре группы и опиши порядок обмена». Класс можно передать как возрастную группу, если он нужен сложности плана; буква класса не нужна. Таблицу с именами и телефонами не отправляют: для общего плана она не нужна. Не засчитывайте замену имён инициалами при сохранённых телефонах. Не требуется загружать сам список, чтобы попросить общий план.

ГОВОРИМ УЧЕНИКАМ

Задача сохранилась: помощнику известны число участников, длительность и порядок встречи. Имена и телефоны участников не помогали составить общий план. В ситуации Веры тоже лучше передать текст «сделай таблицу репетиций» с нужными часами без привязки к человеку, а не отправлять снимок целиком.

05. Этап 3. Знакомый голос и независимая проверка

≈ 12 минут

ГОВОРИМ УЧЕНИКАМ

ИИ может создавать похожие на настоящие изображения и голоса. Такую подделку называют дипфейком. Злоумышленник может использовать её, чтобы выдать себя за знакомого человека. Узнать голос или лицо поэтому недостаточно: важную просьбу проверяют через другой, заранее известный канал связи.

Реальный случай. Видеовстреча с поддельными руководителями

7 февраля 2024 года центр реагирования на компьютерные инциденты HKCERT рассказал о мошенничестве в Гонконге. Сотрудника компании убедили перевести 200 миллионов гонконгских долларов после видеовстречи с поддельными изображениями и голосами руководителей. Этот случай показывает: убедительное изображение ещё не подтверждает личность собеседника.

Как проверить просьбу?

В общем чате кружка появляется сообщение от аккаунта руководителя: «Для новой нейросети нужно подтвердить доступ. Я сейчас позвоню, продиктуй код из сообщения». Через минуту приходит голосовой звонок, голос похож на знакомый. У тебя есть номер руководителя, сохранённый ещё в начале учебного года.

1. Запишите два действия до ответа на просьбу.
2. Объясните, почему вопрос в том же чате не будет независимой проверкой.
3. Предположите, что аккаунт действительно захватили. Какое последствие может иметь передача кода?

Для учителя: ответы и обсуждение

Код не сообщают, разговор прекращают или откладывают. С помощью взрослого связываются с руководителем по заранее известному номеру, не по новому контакту из сообщения. Тот же чат может контролировать тот же злоумышленник. Переданный код может открыть доступ к аккаунту или подтвердить действие, для которого его прислали. Из условия нельзя утверждать, что взлом уже доказан. Засчитывайте осторожность и проверку без объявления любого похожего голоса поддельным.

ГОВОРИМ УЧЕНИКАМ

Мы проверяем источник просьбы, а не пытаемся на слух угадать, настоящий ли голос. Даже знакомый аккаунт может оказаться под чужим управлением. Использование ИИ для обмана остаётся обманом, даже если текст или голос создала программа.

06. Этап 4. Два вида безопасности и первый шаг ≈ 11 минут

ГОВОРИМ УЧЕНИКАМ

Цифровая безопасность защищает данные, аккаунты и устройства. Физическая безопасность защищает жизнь и здоровье. Один ответ может затрагивать обе: публикация точного расписания с адресом связывает человека с местом и временем, а это может затронуть и его личную безопасность. Оценивать нужно последствия, а не только устройство, с которого пришёл ответ.

Если данные уже отправлены, не стоит продолжать передачу, чтобы «проверить, что случится». Сообщите доверенному взрослому, какие именно сведения ушли и куда. Он поможет обратиться в сервис и защитить доступ. Удаление сообщения на экране само по себе не доказывает, что копий нигде не осталось. Если помощник советует опасное действие с веществами, огнём или электричеством, остановитесь и обратитесь к взрослому, который отвечает за эту работу.

Назовите риск и первый шаг

А. Ученик выбрал для аватара фото у подъезда: ему нравится освещение. На фоне видна табличка с улицей и номером дома.

Б. Помощник предлагает ускорить уборку, соединив два бытовых чистящих средства.

В. Ученик уже отправил файл со списком телефонов группы и заметил это после ответа.

1. Для каждой карточки запишите возможное последствие и безопасный первый шаг.
2. Укажите, какой риск цифровой, физический или относится к обоим видам. Объясните выбор для одной спорной карточки.

Для учителя: ответы и обсуждение

А: лицо и табличка позволяют связать человека с местом, поэтому возможны цифровой и физический риски. Снимок у подъезда не доказывает, что ученик живёт в этом доме, но передавать лишнюю привязку к месту для аватара не нужно. Можно выбрать изображение без таблички или рисунок. Б: физический риск; не смешивать и обратиться к взрослому. Ученики не перечисляют составы и не проводят опыт. В: цифровой риск; остановить передачу и сообщить доверенному взрослому, указав сервис и отправленный файл. Не утверждайте, что утечка точно произошла: известно о передаче, а доступ посторонних неизвестен. Пункт о смешивании — правило предосторожности, не утверждение, что любая пара средств даёт одинаковую реакцию.

ГОВОРИМ УЧЕНИКАМ

Разработчики тоже должны защищать сервис: ограничивать доступ к данным, проверять безопасность и понятно объяснять обработку. Пользователь со своей стороны оставляет в запросе только нужные сведения и не выполняет опасные советы. Эти действия дополняют друг друга.

07. Этап 5. Итоги урока ≈ 5 минут

ГОВОРИМ УЧЕНИКАМ

Мы сохранили полезный запрос, не передав лишние данные, и нашли способ проверить подозрительную просьбу. Назовите действие и объясните, какой риск оно уменьшает.

Главное за урок

В запросе оставляют только нужные для задачи сведения. Пароли и одноразовые коды не передают. Подозрительную просьбу проверяют по заранее известному контакту, а об ошибочной передаче данных сообщают доверенному взрослому.

Итоговые вопросы

1. Почему удалить фамилию со снимка иногда недостаточно?
2. Какие условия оставить в запросе о плане встречи?
3. Как проверить просьбу знакомого голоса о коде?
4. Что делать, если файл с чужими телефонами уже отправлен?

Для учителя: ответы и обсуждение

1. Остальные детали могут вместе определять человека. 2. Только нужные задаче: число участников, время, группы и вид работы. 3. Код не передавать; связаться по заранее известному независимому контакту с помощью взрослого. 4. Остановить дальнейшую передачу и сообщить взрослому, что и куда отправлено, затем с ним защитить доступ и обратиться в сервис. Ответ «просто удалить» неполон.

Для учителя: источники

1. ЮНЕСКО. Рекомендация об этике искусственного интеллекта
   Дата материала: Ноябрь 2021 — принятие рекомендации; у обзорной страницы дата публикации не указана. Проверена 03.11.2026.

   Справедливость, защита данных, прозрачность, ответственность и контроль человека; это этические принципы, а не инструкция к отдельному сервису.

   > AI systems do not displace ultimate human responsibility and accountability.

2. HKCERT. Предупреждение о мошенничестве с поддельной видеоконференцией
   Дата материала: 07.02.2024.

   Случай в Гонконге, подделка голоса и изображения, проверка источника и запрет передачи секретов незнакомому собеседнику.

   > deceived into transferring HK$200 million to five local accounts

3. ЮНЕСКО. Руководство по генеративному ИИ в образовании и исследованиях
   Дата материала: 07.09.2023; обновление обзорной страницы 16.01.2026. Материал старше 2024 года.

   Защита данных и самостоятельности учащегося; выбор применения ИИ с учётом возраста. Правила конкретного задания устанавливает учитель.

   > a human-agent and age-appropriate approach