

OUCH!

Ежемесячный информационный бюллетень по безопасности

Искусственный интеллект: что нужно знать

Что это такое и почему меня это должно волновать?

Искусственный интеллект (ИИ) описывает системы, запрограммированные думать и реагировать как люди. На самом деле, мы задали ИИ-решению ChatGPT именно этот вопрос и получили такой ответ.

Что такое искусственный интеллект?

Искусственный интеллект (ИИ) относится к моделированию человеческого интеллекта в машинах, которые запрограммированы думать и учиться, как люди. Он включает в себя разработку алгоритмов и компьютерных программ, которые могут выполнять задачи, обычно требующие человеческого интеллекта, такие как распознавание речи, понимание естественного языка, принятие решений и игры. Существует несколько типов ИИ, включая ИИ на основе правил, экспертные системы и машинное обучение.

Что делает ИИ таким мощным, так это то, что он может имитировать интеллект и способность рассуждать человеческим разумом, но он может экспоненциально анализировать гораздо больше информации, чем любой человек, и делать это быстрее.

Концепция ИИ не нова. Первоначально описанный в научно-фантастических романах, ИИ разрабатывался десятилетиями. Причина, по которой вы так много слышите об этом сейчас, заключается в том, что впервые у каждого есть возможность взаимодействовать и увидеть истинную функциональность ИИ.

ChatGPT, онлайн-чат-бот с искусственным интеллектом, является одним из первых общедоступных решений, способных реагировать как настоящий человек, пройдя так называемый тест Тьюринга. Этот тест определяет способность машины демонстрировать интеллектуальное поведение, когда реальный человек взаимодействует с машиной через канал текстового чата. Если человек не может сказать, взаимодействовали они с машиной или с человеком, говорят, что машина прошла тест. Решения ИИ на сегодняшний день являются первыми общедоступными решениями, которые делают именно это.

Однако онлайн-разговоры — это только начало того, на что способен ИИ. Сейчас есть ИИ-решения, которые могут создавать видео человека, преподающего урок на любом языке, анализировать медицинские записи и быстро определять, у кого, скорее всего, рак, создавать новостные статьи или эссе на выбранную вами тему, генерировать изображения для детских книг, или создать код для новых компьютерных программ. Хотя ИИ не обязательно является чем-то, чего следует опасаться, существуют некоторые опасности, о которых следует знать.

Опасности искусственного интеллекта

1. **Воссоздание вас:** решения ИИ могут записывать голос человека — ваш голос — и затем использовать его для создания звука в реальном времени, который звучит так же, как вы, говоря все, что хочет, чтобы выдать себя за вас. Таким образом, кибер-злоумышленник может записать телефонное голосовое сообщение, которое звучит как вы, обманывая ваших коллег, ваш банк или члена семьи, заставляя их думать, что вы звонили и просили их предпринять какие-либо действия. ИИ также может делать это с изображениями или видео. Иногда называемое Deep Fakes, ИИ-решение может взять существующее изображение или видео с вами и использовать его для воссоздания совершенно новых изображений или видео (включая ваш голос), чтобы показать, как вы делаете то, чего никогда не делали.
2. **Неправильные ответы:** что касается данных или ответов, которые предоставляет ИИ, решения могут быть неверными. ИИ часто использует общедоступную информацию из Интернета, и на его ответы могут влиять предубеждения его разработчиков. В то время как типичные поисковые системы предназначены для предоставления вам «лучших» или наиболее правильных ответов на ваши запросы, такие решения, как ИИ, могут быть разработаны, чтобы давать вам ответы, максимально приближенные к человеческим. Что лучше, зависит от того, чего вы пытаетесь достичь.
3. **Не все равны:** ИИ становится новейшей популярной технологией, и теперь буквально сотни стартапов предлагают различные услуги ИИ. Многим из них нужна ваша информация или кредитная карта для пробной версии. Будьте осторожны — не все сервисы ИИ заслуживают доверия. Проведите исследование, прежде чем регистрироваться и использовать сервис ИИ.
4. **Ваша конфиденциальность:** всякий раз, когда вы используете систему искусственного интеллекта или взаимодействуете с ней, например, при онлайн-чате с ChatGPT, помните, что любая информация, которую вы вводите в систему, может не только обрабатываться ею, но также сохраняться и использоваться для предоставления ответов другим. Это означает, что если вы введете какую-либо личную информацию о себе или любую конфиденциальную информацию с работы, эта информация будет сохранена и потенциально передана или продана другим лицам. Не делитесь и не вводите какую-либо информацию, которую вы считаете конфиденциальной, личной или конфиденциальной на работе.

Будущее ИИ

Искусственный интеллект все еще находится в зачаточном состоянии, подобно тому, каким был Интернет двадцать-тридцать лет назад. Хотя мы можем ожидать быстрого развития и внедрения ИИ, очень сложно предсказать, каким будет его влияние. Просто имейте в виду, что эти возможности существуют, и при использовании ИИ будьте очень осторожны с информацией, которую вы вводите и которой делитесь.

Ресурсы

ChatGPT: <https://chat.openai.com/chat>

Тест Тьюринга: https://en.wikipedia.org/wiki/Turing_test

Роман Полаков

OUCH! Публикуется SANS Security Awareness и распространяется под лицензией [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Вы можете делиться или распространять этот информационный бюллетень, если вы не продаете и не модифицируете его. Редакционная коллегия: Уолтер Скriverенс, Фил Хоффман, Алан Ваггонер, Лесли Ридаут, Принцесса Янг.