Министерство науки и высшего образования Российской Федерации
Калужский филиал федерального государственного автономного образовательного учреждения высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(КФ МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ ИУК Информатика и управление

КАФЕДРА ИУК9 Иностанные и русские языки

ДОМАШНЯЯ РАБОТА

«Deepfakes»

по дисциплине: «*Иностанный язык*»

Выполнил: студент группы ИУК5-62Б _____ Ли Р. В.
(Подпись) (И.О. Фамилия)

Проверил: _____ Гаврикова Л. Г.
(Подпись) (И.О. Фамилия)

Дата сдачи (защиты):

Результаты сдачи (защиты):

- Балльная оценка:
- Оценка:

Калуга, 2025

In an age where digital manipulation has become increasingly sophisticated, knowing how to spot a deepfake is crucial for safeguarding yourself and others online. Deepfake technology has revolutionized the creation of synthetic media, raising concerns about the authenticity of content in various spheres. With the ability to seamlessly manipulate videos and audio, deepfakes pose significant threats to individuals, businesses, and society. Just ask celebrities such as Taylor Swift and Mr. Beast, who have been victimized by deepfake technology. In this blog post, we'll delve into what deepfakes are, how they work, their potential dangers, and their legal implications. And, most importantly, how you can spot them to safeguard yourself and others. **What Is a Deepfake?** Deepfakes are synthetic media in which a person in an existing image or video is replaced with someone else's likeness using advanced machine-learning	В эпоху, когда цифровые технологии манипуляции становятся всё более продвинутыми, умение распознавать дипфейки крайне важно для защиты себя и других в интернете. Технология дипфейков кардинально изменила создание синтетических медиа, вызывая серьёзные сомнения в подлинности контента в самых разных сферах. Благодаря способности правдоподобно изменять видео и звук, дипфейки представляют серьёзную угрозу для частных лиц, компаний и общества в целом. Об этом могут рассказать такие знаменитости, как Тейлор Свифт и Mr. Beast, которые уже пострадали от этой технологии. В этом посте мы разберёмся, что такое дипфейки, как они работают, чем опасны и какие юридические последствия могут иметь. И, что самое главное — как их распознать, чтобы обезопасить себя и окружающих. **Что такое дипфейк?** Дипфейк — это синтетический медиафайл, в котором человек на изображении или в видео заменяется на

algorithms. These manipulated videos or audio recordings can be incredibly convincing, often indistinguishable from authentic content.

There are many types of deepfakes, such as:

- **Face swapping.** This occurs when another person's face replaces the face of the original person.
- **Lip synchronization.** This is where the mouth of someone speaking is modified by an audio track, making the voice different from the original.
- **Voice cloning.** Here, a voice is copied to use that voice somewhere else.

How Do Deepfakes Work?

Deepfake technology utilizes deep learning algorithms, particularly generative adversarial networks (GANs), to analyze and mimic facial expressions, voice tones, and mannerisms. By training on vast datasets of images and videos, these algorithms can generate highly realistic simulations of individuals, allowing malicious actors to create convincing fake

другого человека с помощью продвинутых алгоритмов машинного обучения. Такие поддельные видео или аудио могут быть настолько реалистичными, что их почти невозможно отличить от настоящих.

Существует несколько видов дипфейков, например:

- **Замена лица (face swapping)** — лицо одного человека заменяется лицом другого.
- **Синхронизация губ (lip sync)** — движения рта человека подгоняются под другой аудиотрек, создавая иллюзию другого голоса.
- **Клонирование голоса (voice cloning)** — голос копируется и используется в других местах.

Как работают дипфейки?

Технология дипфейков использует алгоритмы глубокого обучения, особенно так называемые генеративные состязательные сети (GANs), чтобы анализировать и копировать мимику, интонации и поведение. Обучаясь на

content. **Why Are Deepfakes Dangerous?** The proliferation of deepfake technology presents numerous risks, including misinformation, defamation, and privacy violations. Deepfakes have the potential to spread false narratives, manipulate public opinion, and even incite violence or unrest. Moreover, they can be used to impersonate individuals, leading to reputational damage or financial losses. **Are Deepfakes Illegal?** The legality of deepfakes varies depending on jurisdiction and the context in which they are used. Let's explore the deepfake situation in the United States and the United Kingdom. **United States** In the United States, laws regarding deepfakes are still evolving, with limited federal legislation specifically addressing the issue. However, existing laws related to fraud, defamation, and intellectual property rights may apply to specific deepfake scenarios. In January 2024, representatives	огромных массивах данных — изображениях и видео, — эти алгоритмы создают правдоподобные симуляции людей, что позволяет злоумышленникам подделывать контент, выглядящий очень убедительно. **Почему дипфейки опасны?** Распространение дипфейков несёт множество рисков: от дезинформации и клеветы до нарушений частной жизни. Такие видео могут распространять ложные идеи, манипулировать общественным мнением и даже провоцировать насилие или беспорядки. Также их можно использовать для имитации личности, что может нанести вред репутации или привести к финансовым потерям. **Являются ли дипфейки незаконными?** Законность дипфейков зависит от страны и контекста их использования. Рассмотрим ситуацию в США и Великобритании.

proposed the No Artificial Intelligence Fake Replicas And Unauthorized Duplications Act. The bill establishes a federal framework to protect individuals against Artificial Intelligence-generated fakes by making it illegal to create digital depictions of any person, dead or alive, without their permission.

The US has also proposed the following:

- The Senate's Nurture Originals, Foster Art, and Keep Entertainment Safe (NO FAKES) Act, would protect the performers' voice and visual likeness.
- The Disrupt Explicit Forged Images and Non-Consensual Edits (DEFIANCE) Act would allow people to sue over faked pornographic images of themselves.

As the US is decentralized, some individual US states have already taken action or are in the process of doing so against deepfake technology. However, the current laws vary in many ways depending on the state. This includes the definition of deepfakes and the type of liability they impose. States that target deepfake content

США

В США законы о дипфейках всё ещё находятся в стадии разработки, и на федеральном уровне пока что нет чёткой регуляции. Однако уже существующие законы — о мошенничестве, клевете или нарушении авторских прав — могут применяться в определённых ситуациях. В январе 2024 года был предложен законопроект *No Artificial Intelligence Fake Replicas And Unauthorized Duplications Act*, который создаёт правовую защиту от ИИ-подделок и запрещает создавать цифровые копии людей без их разрешения.

Также были предложены:

- **NO FAKES Act** — защищает голос и внешний облик артистов.
- **DEFIANCE Act** — позволяет подавать в суд за поддельные порнографические изображения.

Так как США — децентрализованное государство, некоторые штаты уже приняли собственные законы против дипфейков. Но они сильно отличаются:

include Florida, Georgia, Hawaii, and Illinois, to name a few.

Let's explore two states that took early action against deepfakes.

California Deepfake Law

In the realm of AI regulation within the United States, California stands as a pioneer. Notably, its enactment of the California deepfake law marked one of the earliest instances nationwide, commencing in 2019. This legislation not only renders non-consensual deepfake pornography a criminal offense but also grants victims the capacity to pursue legal action against individuals who fabricate images utilizing their likenesses (under Assembly Bill 602). Furthermore, it prohibits the utilization of AI-generated deepfakes during election campaigns, as outlined in Assembly Bill 730.

Texas Deepfake Law

The Lone Star state of Texas took an early stance in the United States by enacting legislation, specifically, Senate Bill 751, aimed at curtailing the creation and dissemination of videos with the intent to

как по определению дипфейков, так и по видам ответственности. Например, такие штаты, как Флорида, Джорджия, Гавайи и Иллинойс, уже работают над этим вопросом.

Вот два примера:

Калифорния:
Законодательство штата считается одним из самых ранних и прогрессивных. С 2019 года действует закон, запрещающий использование дипфейков в порнографии без согласия и в избирательных кампаниях. Пострадавшие могут подавать иски против тех, кто использует их изображения (Assembly Bill 602 и Assembly Bill 730).

Техас:
Штат принял закон Senate Bill 751, запрещающий создание дипфейков с целью повлиять на выборы. Также действует закон, запрещающий распространение порнографических дипфейков без согласия.

Великобритания

В Великобритании создание и

manipulate or interfere with elections. Subsequently, Texas further fortified its legal framework concerning deepfake technology by implementing the Unlawful Production or Distribution of Certain Sexually Explicit Videos law. This statute criminalizes the production of explicit deepfake videos without the consent of the individuals depicted therein. **United Kingdom** In the United Kingdom, creating and distributing deepfakes with malicious intent could potentially violate laws related to fraud, harassment, or privacy infringement. The UK government is also considering legislative measures to combat the spread of harmful deepfake content. In 2023, Britain enacted the UK Online Safety Act. This Act prohibits disseminating manipulated explicit content under circumstances where it deliberately or negligently inflicts harm upon an individual. However, the Act doesn't extend to the prohibition of pornographic deepfakes, nor does it restrict their sharing unless there is clear evidence of intent to	распространение дипфейков с вредоносными намерениями может нарушать законы о мошенничестве, домогательствах или вторжении в личную жизнь. В 2023 году был принят **UK Online Safety Act**, который запрещает публикацию поддельного откровенного контента, если есть цель причинить вред. Однако этот закон не запрещает дипфейки порнографического характера или их распространение, если не доказан умысел нанести вред. Также в стране пока нет закона, прямо запрещающего создавать ИИ-контент без согласия изображаемого человека. В таких случаях можно опираться на нормы о клевете, защите данных, авторском праве и другие. Но доказать такие нарушения часто бывает сложно.

cause distress. Additionally, the amendments don't criminalize the creation of other AI-generated media without the subject's consent. In such cases, individuals whose likeness has been exploited for malicious purposes may seek recourse through defamation, privacy laws, harassment statutes, data protection regulations, intellectual property rights, or other applicable criminal statutes. However, these can often be intricate and challenging to substantiate.	

Вопросы

1. How deepfake technology manages to create such realistic videos.
2. Why deepfakes are seen as a threat to individuals and society.
3. What legal measures different countries have taken against deepfakes.
4. How GANs contribute to the generation of synthetic media.
5. What consequences deepfakes could have during political campaigns.
6. Whether current laws are enough to regulate the use of deepfakes.
7. How people can learn to identify a deepfake.
8. What risks are involved in the use of voice cloning and face swapping.
9. How celebrities have been affected by deepfake content.
10. What challenges victims face when trying to seek justice for deepfake misuse.

Реферат

В статье "Deepfake: What It Is and How to Spot One", опубликованной в блоге компании Surfshark в 2024 году, рассматриваются ключевые аспекты, связанные с технологией дипфейков. Автором материала выступает команда Surfshark Security Team. Основное внимание уделяется описанию самого явления, его возможных последствий, а также законодательным мерам, предпринимаемым для борьбы с этим видом фальсификаций. Дипфейк — это синтетический медиафайл, созданный с помощью искусственного интеллекта, который может подделывать внешность, голос и действия человека, делая их почти неотличимыми от реальности. Статья подчёркивает, что с развитием технологий возрастает риск их злонамеренного использования — в политике, мошенничестве, порочащих кампаниях и других сферах. Анализируются законодательные инициативы, принятые в США (например, NO FAKES Act, DEFIANCE Act) и Великобритании (в том числе Online Safety Act), с акцентом на то, что правовое регулирование пока отстаёт от темпов технологического прогресса. Автор приводит конкретные примеры, связанные с публичными личностями, чтобы показать актуальность проблемы. В статье также содержатся рекомендации, как распознавать дипфейки и повышать цифровую грамотность. Делается вывод, что на фоне растущей угрозы необходимо не только совершенствовать законодательство, но и повышать осведомлённость граждан. В целом, работа представляет собой краткий обзор проблемы, освещая как техническую, так и правовую стороны вопроса, подводя читателя к пониманию того, что борьба с дипфейками — это общая задача общества, государства и технологических компаний.