ЦИФРОВАЯ ЭКОНОМИКА
D-ECONOMY.RU

Автономная некоммерческая организация «Цифровая экономика»

123112, Москва, Пресненская набережная, д.10, блок В, 10 этаж

office@data-economy.ru
+7 (495) 587-04-77

d-economy.ru

Автономная некоммерческая организация
«ЦИФРОВАЯ ЭКОНОМИКА»

«Кибербезопасность и искусственный интеллект»

Методические рекомендации

по организации и проведению в школах Российской Федерации тематических занятий дополнительного образования в рамках Всероссийской образовательной акции «Урок цифры»

Авторы-составители:

Сиденко Андрей Григорьевич, руководитель направления по детской онлайн-безопасности, абсолютный победитель конкурса «Учитель года России 2013»

Москва, 2024

Содержание

Оглавление

Аннотация

- Цель и назначение рекомендаций.
- Значение кибербезопасности и ИИ в образовании.
- Роль технологии искусственного интеллекта в профессиональном и личностном развитии.

Методические рекомендации разработаны для поддержки педагогов и родителей в проведении тематического занятия по теме «Кибербезопасность и искусственный интеллект» в рамках Всероссийской образовательной акции «Урок цифры». Акция «Урок цифры» носит просветительский и профориентационный характер, способствуя осознанию важности защиты данных в цифровом мире и использования искусственного интеллекта для обеспечения кибербезопасности. Изучение кибербезопасности и связанных с ней технологий актуально как никогда, так как цифровизация охватывает все аспекты жизни, включая учебу, работу и повседневную деятельность. Эти знания становятся универсальными и необходимыми для всех профессий и образовательных направлений. Формирование таких навыков требует понимания технологий, развития критического мышления и внимательного отношения к вопросам безопасности.

Методические рекомендации по теме «Кибербезопасность и искусственный интеллект» разработаны для проведения занятий с обучающимися 1-4, 5-9 и 10-11 классов с учетом возрастных особенностей. На занятии школьники изучат, как киберпреступники используют искусственный интеллект для реализации фишинговых атак, распространения вредоносного ПО, создания дипфейков и других угроз, с которыми можно столкнуться в цифровом мире. Учащиеся освоят, как можно распознавать такие угрозы, защитить себя и свои данные, а также вычислять злоумышленников, применяя основы кибербезопасности и технические средства защиты информации. Практическая часть занятия включает работу с интерактивными тренажерами, которые помогут закрепить навыки выявления подозрительных действий в сети и познакомят с инструментами для анализа данных и предотвращения угроз. Цель

занятия — мотивировать школьников осваивать навыки кибербезопасности, необходимые для уверенного взаимодействия с современными цифровыми технологиями.

Методические рекомендации по теме «Кибербезопасность и искусственный интеллект» будут полезны учителям, классным руководителям, педагогам дополнительного образования, представителям администрации образовательных учреждений, студентам педагогических вузов и колледжей. Материалы также помогут родителям познакомить детей с основами кибербезопасности и начать применять эти знания в своей профессиональной и личной жизни.

Методические рекомендации разработаны на основе успешного опыта российских образовательных проектов, включающих обучение кибербезопасности и искусственному интеллекту.

1. Урок цифры (2018–2025 гг.) — федеральная образовательная акция, охватывающая темы безопасного поведения в интернете, работы с данными и искусственным интеллектом [Электронный ресурс]. URL: https://урокцифры.рф/ (дата обращения: 10.10.2024).

2. Академия искусственного интеллекта для школьников — проект, направленный на обучение навыкам работы с ИИ, включая распознавание угроз и безопасное использование технологий [Электронный ресурс]. URL: https://ai-academy.ru/ (дата обращения: 10.10.2024).

3. Кружковое движение НТИ — инициатива, развивающая проектные и исследовательские навыки школьников в области технологий и науки [Электронный ресурс]. URL: https://kruzhok.org/ (дата обращения: 10.10.2024).

4. Национальная технологическая олимпиада (НТО) — соревнование для школьников 8–11 классов, которое включает направления, связанные с цифровыми технологиями и искусственным интеллектом [Электронный ресурс]. URL: https://ntcontest.ru/tracks/nto-school/ (дата обращения: 10.10.2024).

5. НТО.Junior — аналог олимпиады НТО для учащихся 5–7 классов, с акцентом на практическое применение знаний по кибербезопасности и работе с ИИ [Электронный ресурс]. URL: https://junior.ntcontest.ru/#spheres (дата обращения: 10.10.2024).

6. Безопасный интернет от Фонда Развития Интернет-Инициатив (ФРИИ) — образовательные программы по киберграмотности и защите данных [Электронный ресурс]. URL: https://www.iidf.ru/media/articles/trends/kiberprestupnost-v-rossii-ugrozy-masshtaby-sredstva-borby/, http://detionline.com/video/professional/ (дата обращения: 10.10.2024).

7. Яндекс.Учебник — материалы по обучению цифровым навыкам, включая анализ данных и основы безопасного взаимодействия с технологиями [Электронный ресурс]. URL: https://education.yandex.ru/ (дата обращения: 10.10.2024).

8. Сириус — образовательный центр, предлагающий курсы и мероприятия для школьников по темам ИИ, кибербезопасности и программирования [Электронный ресурс]. URL: https://sochisirius.ru/ (дата обращения: 10.10.2024).

9. Российская программа “Цифровая образовательная среда” (Федеральный проект «Цифровая образовательная среда») — инициативы, поддерживающие использование цифровых инструментов и технологий в образовательном процессе [Электронный ресурс]. URL: https://edu.gov.ru/projects/cos (дата обращения: 10.10.2024).

10. Курсы “Точки роста” — образовательные центры в школах, где дети обучаются цифровым навыкам, включая безопасное использование интернета и технологий [Электронный ресурс]. URL: https://mpcenter.ru/national-project/informacionnoe-soprovozhdenie/tochka-rosta/ (дата обращения: 10.10.2024).

11. Проект “Киберкультура” от Российской Ассоциации электронных коммуникаций (РАЭК) — программы по развитию цифровой грамотности и культуры безопасного общения в интернете [Электронный ресурс]. URL: https://forumsoc.ru/cyberbez-tv/ (дата обращения: 10.10.2024).

Материалы тематического занятия «Кибербезопасность и искусственный интеллект» размещены на сайте акции «Урок цифры» в открытом доступе. Они могут быть использованы для проведения внеурочных занятий, классных часов, профориентационных мероприятий, мастер-классов и других образовательных мероприятий.

Терминология

Ниже перечислены термины и их определения, которые используются в профессиональной среде. Для обучающихся 10-11 классов они не должны вызывать трудности в понимании. Для обучающихся 1-4 класса и старше определения могут быть не всегда понятны. Поэтому в скобках добавлены разъяснения терминов простыми словами, что не является определением.

1. **Алгоритмы машинного обучения (ML)** – методы, позволяющие ИИ обучаться на основе данных для выполнения задач. (Это когда компьютеры учатся, как решать задачи, на основе примеров.)
2. **Антивирус** – программное обеспечение для защиты устройства от вредоносных программ. (Это программа, которая защищает твой компьютер от вирусов и других опасных программ.)
3. **Аутентификация** – процесс подтверждения личности пользователя, например, через пароль или биометрические данные. (Это как проверка, кто ты, например, через пароль или отпечаток пальца.)
4. **Вредоносное ПО (malware)** – программы, которые наносят вред устройствам, крадут данные или нарушают их работу. (Это программы, которые могут сломать твой компьютер или украсть твою информацию.)
5. **Data Scientists (Специалисты по данным)** – профессионалы, которые анализируют большие массивы данных для выявления закономерностей, слабых мест в системах и для разработки решений для их улучшения. (Это люди, которые ищут важную информацию в данных, чтобы помочь сделать систему или сервис лучше.)

6. **Дипфейк** – технология, позволяющая создавать поддельные видео, аудио, а также изображения с использованием искусственного интеллекта. Может быть использована для обмана или манипуляции. (Это когда создают фальшивые видео или картинки, которые могут тебя обмануть.)

7. **Злоумышленник** – человек, который намеренно причиняет вред другим, использует мошеннические схемы или нарушает закон. (Это плохой человек, который делает что-то вредное или незаконное.)

8. **HTTPS-протокол** – защищенное соединение, используемое для обеспечения безопасности передачи данных в интернете. (Это специальная защита, которая помогает сохранять твою информацию в безопасности, когда ты заходишь на сайт.)

9. **Искусственный интеллект (ИИ)** – технологии, которые имитируют человеческое мышление и способность к обучению. (Это когда компьютер может учиться и думать, как человек.)

10. **Кибербезопасность** – комплекс мер и технологий, направленных на защиту данных и систем от киберугроз. (Это как защита для твоего компьютера и телефона от вирусов и хакеров.)

11. **Конфиденциальность** – защита личной информации от несанкционированного доступа. (Это право на то, чтобы твоя личная информация была в безопасности и никто не мог ее украсть.)

12. **Логин** – имя пользователя, которое используется для доступа к аккаунту или сервису. (Это твое имя для входа в аккаунт на сайте или в программе.)

13. **Личные данные** – информация, которая может идентифицировать человека (например, имя, адрес, дата рождения). (Это информация о тебе, например, твое имя или адрес.)

14. **Манипуляции (в рамках социальной инженерии)** – методы давления, такие как запугивание, создание срочности или обещание награды. (Это когда тебя пытаются заставить сделать что-то, используя хитрые приемы, например, запугивание или обещание чего-то ценного.)

15. **ML-инженеры** – специалисты, которые разрабатывают системы искусственного интеллекта, способные обучаться на данных, извлекая закономерности для выполнения различных задач, включая предсказание угроз и улучшение безопасности. (Это люди, которые создают компьютеры, которые учат сами себя, чтобы они могли решать разные задачи.)

16. **Навязчивая реклама** – рекламный контент, который появляется без согласия пользователя и отвлекает внимание. (Это когда реклама появляется постоянно и мешает тебе работать или играть.)

17. **Облачные сервисы** – удаленные платформы для хранения и обработки данных. (Это как большой виртуальный шкаф, где можно хранить информацию и получать к ней доступ через интернет.)

18. **Обработка данных** – процесс сбора, хранения и использования персональной информации. (Это когда кто-то собирает и использует твою личную информацию, например, для улучшения сервиса.)

19. **Песочница (sandbox)** – виртуальная среда для безопасного тестирования подозрительных файлов или программ. (Это как безопасная комната, где можно проверить, не опасен ли файл или программа, не повредив компьютер.)

20. **Поддельные логотипы и изображения** – низкокачественные графические элементы, используемые для имитации официальных брендов. (Это когда делают фальшивые картинки, чтобы обмануть людей.)

21. **Подозрительные URL-адреса** – интернет-ссылки с неестественными символами или доменами, которые часто используются для фишинга. (Это странные ссылки на сайты, которые могут быть опасными.)

22. **Социальная инженерия** – метод манипуляции людьми с целью получить доступ к их данным или системе. (Это когда кто-то обманывает тебя, чтобы ты рассказал секреты или передал важную информацию.)

23. **Специалист по кибербезопасности** – профессионал, который занимается защитой информации и систем от хакеров и злоумышленников, обеспечивая безопасность паролей и других данных. (Это человек, который защищает твой компьютер и данные от хакеров и вирусов.)

24. **Утечка данных** – несанкционированное раскрытие или доступ к личной информации. (Это когда твоя личная информация попадает в чужие руки без твоего разрешения.)

25. **Фишинг** – форма интернет-мошенничества, при которой злоумышленники пытаются получить конфиденциальную информацию обманным путем. (Это когда люди пытаются обмануть тебя, чтобы получить твои пароли или деньги.)

26. **Чат-боты** – программы с искусственным интеллектом, предназначенные для общения с пользователями. (Это как роботы, которые могут общаться с тобой через текст или голос.)

Введение

Тема кибербезопасности и искусственного интеллекта (ИИ) становится особенно актуальной в современном мире. В условиях цифровизации и повсеместного использования интернет-технологий защита данных и личной информации становится важной частью жизни каждого человека. Образование играет ключевую роль в формировании у школьников навыков безопасного взаимодействия с технологиями, а также в воспитании культуры ответственного и этичного использования искусственного интеллекта.

Правильно настроенные алгоритмы ИИ могут: выявлять угрозы, анализировать данные о безопасности компьютерной системы, помогать предотвращать кибератаки, защищать конфиденциальную информацию и помогать с решением задач, связанных с безопасностью. Он может учиться на примерах, к которым у алгоритма ИИ есть доступ, улучшая свои способности с каждым днем. Однако, несмотря на все положительные стороны, ИИ может быть использован и злоумышленниками для реализации мошеннических схем, таких как фишинг. Например, с помощью ИИ можно создавать поддельные письма или сайты, которые выглядят как настоящие и обманывают пользователей, заставляя их передавать личные данные или устанавливать вредоносное ПО.

В рамках образовательной акции «Урок цифры» в 2025 году выбрана актуальная тема занятия — «Кибербезопасность и искусственный интеллект». На занятии обучающимся 1–11 классов будет продемонстрировано, как использовать искусственный интеллект для обеспечения безопасности в интернете, как распознавать угрозы, защищать данные и работать с инструментами ИИ, которые помогают в защите от киберугроз. Также будут рассмотрены примеры того, как злоумышленники используют ИИ для создания фальшивых сервисов и поддельных материалов с целью обмана пользователей. На практике школьники смогут освоить основы защиты информации с помощью ИИ и научиться принимать меры безопасности в реальных ситуациях.

Мы находимся на этапе формирования правил взаимодействия человека с искусственным интеллектом в области кибербезопасности. Педагогам и родителям важно воспитывать у детей культуру безопасного и осознанного взаимодействия с цифровыми технологиями, формировать этику и ответственность в вопросах безопасности, а также прививать знания, которые помогут им эффективно защищать свою информацию и личные данные.

ИИ может значительно повысить уровень защиты данных и автоматизировать процессы, но он не заменит человеческий фактор. В будущем важность знаний в области кибербезопасности, критического мышления, креативности и умения работать с новыми технологиями будет только расти. Однако важно понимать, что ИИ может быть использован не только для защиты, но и для атак, и уметь распознавать такие угрозы будет важным навыком для каждого. Обучать основам кибербезопасности необходимо в связке с развитием информационной культуры и нравственных ценностей, которые помогут детям и подросткам осознавать важность защиты данных и ответственности за их безопасность. Указ Президента РФ от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» подчеркивает важность формирования нравственных ориентиров, которые лежат в основе безопасности в цифровом мире, укрепляя гражданскую идентичность и

Методические материалы для организации и проведения занятия по теме «Кибербезопасность и искусственный интеллект» для обучающихся 1-4, 5-9 и 10-11 классов помогут подготовиться и провести занятие как педагогам, так и родителям.

Занятие по теме «Кибербезопасность и искусственный интеллект» можно проводить не только во время акции «Урок цифры», но и в рамках любых внеурочных мероприятий, таких как фестивали, дни технологий и научные праздники. Занятие также может быть проведено в системе начального профессионального образования (СПО), используя методические рекомендации для проведения занятия для 10–11 классов. Важно, что содержание учебных пособий, применяемых в образовательных учреждениях, должно учитывать стремительно развивающиеся технологии и инструменты ИИ, и потребность в формировании знаний и навыков в области кибербезопасности и ИИ. Для участия обучающихся во Всероссийской образовательной акции «Урок цифры» рекомендуется выделить 1 час внеурочной деятельности единоразово на занятие по одному из следующих направлений в соответствии с ФГОС начального общего и основного общего образования:

- актуальные социальные, нравственные проблемы современного мира;
- профориентация школьников;
- формирование функциональной грамотности школьников.

Цель внеурочного занятия, например, по направлению профориентация — формирование готовности школьников к осознанному выбору направления продолжения своего образования и своей будущей профессии, осознание ими важности получаемых в школе знаний для дальнейшей профессиональной и учебной деятельности, развитие их ценностного отношения к труду как основному способу достижения жизненного благополучия и ощущения уверенности в завтрашнем дне. Данная цель коррелирует с целью, которую ставит образовательная акция «Урок цифры» по теме «Кибербезопасность и искусственный интеллект».

Такая потребность может быть реализована в рамках внеурочной деятельности на занятиях по теме «Кибербезопасность и искусственный интеллект» в рамках Всероссийской акции «Урок цифры».

Образовательная организация должна обеспечить обучающимся до 10 часов еженедельных занятий внеурочной деятельностью («Письмо Минпросвещения России от 05.07.2022 N ТВ-1290/03 «О направлении методических рекомендаций»). Эти часы могут быть использованы на социальное, творческое, интеллектуальное, общекультурное развитие школьников. Обязательным условием организации внеурочной деятельности является ее воспитательная направленность.

Основная цель занятия по теме «Кибербезопасность и искусственный интеллект» Всероссийской образовательной акции «Урок цифры» — формирование у обучающихся знаний, навыков, культуры и этики безопасного взаимодействия с искусственным интеллектом и цифровыми технологиями, с акцентом на защиту информации и личных данных.

Содержание материалов занятия поддерживает у обучающихся развитие ключевых навыков XXI века:

Критическое мышление. Процесс анализа угроз и защиты данных требует внимательного подхода, умения оценивать риски и принимать обоснованные решения.

Творчество и креативность. Работа с ИИ и киберугрозами развивает креативный подход к решению задач в области цифровой безопасности.

Коммуникативные навыки. Умение ясно и четко формулировать запросы для ИИ, а также обсуждать вопросы безопасности и защиты данных.

Цифровая грамотность. Понимание работы ИИ в сфере кибербезопасности и умение использовать инструменты для защиты данных.

Интерактивные задания и игровые формы при работе с ИИ повышают интерес к обучению и безопасности в интернете. Применение искусственного интеллекта в защите данных и выявлении угроз открывает новые возможности для творчества и обучения, стимулируя интерес к темам кибербезопасности и технологий. Эти задания знакомят с этическими

нормами работы с ИИ и формируют ответственное отношение к возможным последствиям взаимодействия с цифровыми технологиями.

Задачи занятия:

- Сформировать устойчивое понимание терминов, которые вводятся в уроке.
- Дать представление о современных угрозах в интернете и технологиях ИИ, которые помогают их предотвратить.
- Познакомить с общими принципами технологий и алгоритмов, которые уравновешивают спрос и предложение.
- Научить распознавать киберугрозы, такие как фишинг, мошенничество с использованием ИИ и другие угрозы безопасности.
- Обсудить этические аспекты работы с ИИ, особенно в контексте безопасности и защиты личных данных.
- Развить навыки, необходимые для эффективной работы с ИИ в контексте кибербезопасности, включая формулирование запросов и оценку их результатов.
- Провести профориентацию в области кибербезопасности и ИИ.[1]

Указ Президента РФ от 9 ноября 2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» определяет государственную политику в области духовно-нравственного воспитания. Для реализации этого указа на занятии по теме «Кибербезопасность и искусственный интеллект» по возрастным категориям можно решать следующие духовно-нравственные цели:

1-4 классы

Формирование установки на безопасное поведение в сети, развитие чувства ответственности за личную информацию и данные, воспитание осознанного отношения к цифровой безопасности.

[1] Актуально для урока 10-11-х классов

5-9 классы

Формирование ответственного отношения к использованию интернета и технологий, развитие критического мышления при оценке цифровых угроз, формирование нравственных основ для безопасного и этичного общения в интернете.

10-11 классы

Формирование мировоззрения, соответствующего современным вызовам в сфере кибербезопасности и технологий, развитие навыков работы с цифровыми инструментами, воспитание культуры безопасности и ответственности за информацию.

Ожидаемые результаты:

Для обучающихся 1-4 классов основным результатом будет:

- знакомство с основами безопасности в интернете, понимание, что такое киберугрозы и как их избежать, а также навыки формирования простых запросов для ИИ;
- формирование уважительного отношения к духовно-нравственной культуре своей семьи, семейным ценностям;
- формирование уважительного отношения к труду, людям труда, бережного отношения к результатам труда;
- формирование интереса к разным профессиям;
- формирование чувства гордости за успехи в развитии технологий в своей стране;
- развитие первоначальных навыков наблюдений, систематизации и осмысления опыта в естественно-научной и гуманитарной областях знания;
- ознакомление с основными правилами безопасного для себя и других людей поведения в информационной среде.

Для обучающихся 5-9 и 10-11 классов ожидаются более сложные результаты, включая:

- формирование ориентированности на создание устойчивой семьи на основе российских традиционных семейных ценностей;

- формирование уважительного отношения к труду, результатам труда, трудовым и профессиональным достижениям своих земляков;
- формирование ориентированности на осознанный выбор сферы трудовой, профессиональной деятельности в российском обществе;
- развитие навыков безопасного поведения в информационной среде;
- развитие способности адаптироваться к меняющимся информационным условиям;
- развитие понимания специфики трудовой деятельности, самообразования и профессиональной самоподготовки в информационном высокотехнологическом обществе, готовность учиться и трудиться в современном обществе);
- знания о достижениях науки и техники;
- развитие навыков использования различных средств познания, накопления знаний о мире (деятельность в информационной, цифровой среде).
- создание более сложных запросов (промптов) для защиты данных;
- анализ и модификация результатов работы ИИ;
- применение полученных знаний для решения реальных задач в области безопасности данных и интернета.

После завершения занятия по теме «Кибербезопасность и искусственный интеллект» обучающиеся должны:

- Проявить интерес к изучению искусственного интеллекта и его применения в кибербезопасности.
- Быть готовыми к дальнейшему изучению и исследованию в области ИИ и защиты данных.

Понимать:

- Что такое кибербезопасность и как ИИ помогает защищать информацию.
- Как взаимодействовать с ИИ безопасно, избегая фишинга и других угроз.

Знать:

- Основные принципы создания запросов для ИИ с целью обеспечения безопасности.
- Базовый синтаксис запросов и их использование в инструментах безопасности.

Уметь:

- Определять типы угроз в интернете и создавать запросы для ИИ для их предотвращения.
- Анализировать и оптимизировать результаты работы ИИ для защиты личной информации.
- Развивать навыки креативного и критического мышления в решении задач безопасности.

Согласно ФГОС основным объектом и предметом оценки метапредметных результатов на занятии по теме «Кибербезопасность и искусственный интеллект» является овладение:

- Универсальными учебными познавательными действиями, включая работу с информацией, анализ угроз и создание решений.
- Универсальными учебными регулятивными действиями, включая планирование и самоконтроль при решении задач безопасности.

Для обучающихся начальной, основной и старшей школы на занятии будут формироваться личностные результаты:

- Ответственное отношение к использованию технологий и защите данных.
- Умение работать с ИИ и оценивать его результаты для предотвращения цифровых угроз.

Основная часть

Организация занятия

Педагог может провести тематическое занятие по теме «Кибербезопасность и искусственный интеллект» для всех возрастных категорий: 1-4, 5-9 и 10-11 классы, но содержание занятия будет дифференцировано с учетом потребностей и возрастных особенностей школьников разных возрастных

категорий. Тематическое занятие, согласно типологии уроков по ФГОС, относится к уроку открытия нового знания и делится на 4 этапа:

1. Организационный этап – постановка цели и задач занятия.
2. Мотивация учебной деятельности, актуализация знаний – просмотр анимационного ролика или презентации.
3. Усвоение новых знаний, проверка понимания и закрепление – интерактивные задания или игра-тренажер.
4. Подведение итогов занятия – рефлексия (устная или письменная, по усмотрению учителя).

Для всех возрастных категорий рекомендуемая длительность занятия составляет 45 минут. Распределение времени на этапы занятия указано в таблице «План занятия». Педагог может варьировать время этапов занятия в зависимости от ситуации.

План занятия

Этап занятия >>	Организационный этап. Постановка цели и задач	Мотивация учебной деятельности обучающихся Этап актуализации знаний	Этап усвоения новых знаний, проверка понимания и закрепление	Этап подведения итогов занятия. Устная или письменная рефлексия
		Анимационный ролик	Игра-тренажер/ Альтернативное задание*	
1–4 кл.	5 минут	15 минут	20 минут	5 минут
5–9 кл.	8 минут	15 минут	15 минут	7 минут
10–11 кл.	8 минут	15 минут	15 минут	7 минут

Анимационный ролик

Анимационный ролик демонстрируется в начале занятия на этапе мотивации и актуализации знаний и длится до 10 минут. Просмотр ролика вводит обучающихся в изучаемую тематику, дает основные определения и показывает, как технологии ИИ используются в области кибербезопасности. В ролике подчеркивается, что ИИ способен анализировать угрозы, защищать данные и предсказывать возможные риски. Но также поднимаются вопросы:

- Как ИИ может помочь защитить мои данные?
- Как узнать, что с ИИ можно доверять?
- Насколько безопасно использовать ИИ для работы с личной информацией?

Ролик дает ответ: ИИ становится незаменимым инструментом для обеспечения безопасности в интернете. Но, несмотря на его возможности, ответственность за использование ИИ и принятие решений остается за человеком. ИИ не заменяет профессионалов, а помогает решать задачи быстрее и эффективнее. Однако важно уметь правильно формулировать запросы и оценивать результаты работы ИИ, чтобы избежать ошибок и рисков.

Для обучающихся 1-4 классов некоторые понятия, встречающиеся в анимационном ролике, могут быть сложны для восприятия, так как абстрактное мышление еще не развито. Текст для детей этого возраста должен быть максимально простым и доступным. Вместо анимационного ролика учитель может использовать специально разработанную презентацию (ссылка на презентацию находится в разделе “Сценарий альтернативных заданий для обучающихся 1-4 классов”).

Обсуждение содержания ролика

Задайте обучающимся вопросы в течение 3–5 минут, прокомментируйте их ответы. Вопросы могут быть следующими:

1–4 классы

1. Почему Миша сначала поверил сообщению от фальшивого организатора?
2. Какие признаки помогли понять, что сообщение было обманом?
3. Что можно сделать, чтобы защитить свои данные в интернете?
4. Как ты думаешь, откуда злоумышленник узнал о концерте и его участниках?

5–8 классы

1. Как злоумышленник использовал ИИ, чтобы обмануть Мишу?

2. Почему важно проверять сообщения и информацию из нескольких источников?

3. Как настройки конфиденциальности помогли защитить личные данные Миши?

4. Как ты думаешь, откуда злоумышленник узнал о концерте и его участниках?

9–11 классы

1. Какие шаги нужно предпринять, чтобы распознать мошенничество, как это сделал Мидори?

2. Как ИИ может быть использован как для помощи, так и для обмана?

3. Какие меры безопасности нужно соблюдать, чтобы защитить свои данные от злоумышленников?

4. Как ты думаешь, откуда злоумышленник узнал о концерте и его участниках?

Домашнее задание

Дайте обучающимся 1-4 классов домашнее задание: зайти на сайт «Урок Цифры», выполнить задания тренажера по теме «Кибербезопасность и искусственный интеллект» и получить сертификат. Раздайте учащимся памятки с инструкциями, как правильно работать с тренажером, а также ссылками на полезные материалы по теме.

Дополнительно попросите детей вместе с родителями проверить настройки конфиденциальности в их аккаунтах или на устройствах, чтобы убедиться, что личная информация надежно защищена.

Сценарий тренажера

1–4 классы (младшие): Подробные этапы тренажера

Этап тренажера	Содержание
1. Введение (Комикс)	Сюжет комикса: Мидори Кума, Скобец и Запятыня обсуждают, почему нельзя делиться личными данными. Они приводят

	пример с подозрительным другом в игре, который пытается выманить адрес, фотографии и другие данные. Герои объясняют, что такие злоумышленники могут использовать эту информацию во вред. Завершается комикс словами: “Берегите свои данные, как свой самый ценный клад!”
2. Щит конфиденциальности	Интерактивное задание: На экране карточки с информацией: “Любимый цвет”, “Домашний адрес”, “Любимое блюдо”. Учащиеся сортируют карточки в категории: “Можно публиковать” и “Нельзя публиковать”. После каждого выбора появляется пояснение, почему этот выбор правильный или ошибочный. Например, “Домашний адрес” — опасно публиковать, а “Любимый цвет” — безопасно.
3. Создание пароля	Практическое задание: Учащиеся выбирают самый надёжный пароль из предложенных (например, “1234”, “A!grdUU_2024”, “Qwerty”). После этого они создают собственный пароль, добавляя буквы, цифры и спецсимволы. Мидори комментирует: “Надёжный пароль — как прочный замок, его сложно сломать!” Например, “A!grd2024” оценивается как надёжный, а “1234” — слабый.
4. Итоговая задача	Настройка приватности профиля: Учащиеся помогают герою выбрать уровень доступа в его аккаунте. На выбор: “Только друзья”, “Только я”, “Открыто для всех”. Если выбран неправильный вариант, Мидори объясняет, почему. Например, для фотографий с друзьями подходит “Только друзья”, а для личных данных — “Только я”.
5. Завершение	Заключение тренажера: Учащиеся получают виртуальный “щит безопасности” и сертификат о прохождении. Также выдается памятка с основными правилами: “Не делитесь личной информацией”, “Создавайте сложные пароли”, “Проверяйте настройки приватности”.
6. Тест	Тест Шаги выполнения: 1. Вопрос 1: Как узнать, что сообщение от друга написал не он? ○ Варианты ответа: a) Он просит личные данные, которые ему итак уже известны. b) Он поздравляет меня с днем рождения. c) Он спрашивает, какая моя любимая игра. ○ Правильный ответ: a) Он просит личные данные, которые ему итак уже известны. 2. Вопрос 2: Какой из этих паролей самый надежный? ○ Варианты ответа: a) 1234 b) A!grdUU_2024 c) abc ○ Правильный ответ: b)) A!grdUU_2024 3. Вопрос 3: Что нужно делать, если незнакомец в интернете просит личную информацию?

	○ Варианты ответа: a) Рассказать ему все, что он хочет узнать. b) Сказать родителям или учителю и не отвечать. c) Поделиться адресом и номером телефона. ○ Правильный ответ: b) Сказать родителям или учителю и не отвечать. 4. Вопрос 4: Какую информацию нужно спрятать за "щит конфиденциальности"? ○ Варианты ответа: a) Мой любимый цвет. b) Мой домашний адрес. c) Моя любимая еда. ○ Правильный ответ: b) Мой домашний адрес. 5. Вопрос 6: Что может вызывать подозрения в общении с поддельным другом? ○ Варианты ответа: a) Он носит очки. b) Он ведет диалог непривычным образом. c) Он играет с тобой в игры. ○ Правильный ответ: b) Он ведет диалог непривычным образом. 6. Вопрос 7: Что нужно делать, если ты понимаешь, что аккаунт друга в интернете — подделка? ○ Варианты ответа: a) Сообщить родителям или учителю. b) Сказать поддельному другу свой адрес. c) Продолжить общаться с ним. ○ Правильный ответ: a) Сообщить родителям или учителю. 7. Вопрос 8: Как правильно поступить, если кто-либо в интернете просит прислать твои личные данные (например, фото документов или фотографии квартиры и т.д.)? • Варианты ответа: a) Не реагировать и сообщить взрослым. b) Сказать ему все, что он просит. c) Поделиться только своим именем. • Правильный ответ a) Не реагировать и поделиться со взрослыми. Результаты теста: • После завершения теста программа оценивает результаты. • Если ребенок отвечает правильно на все вопросы, его хвалят, и Мидори дарит ему виртуальный "щит безопасности". (Пусть Ваня нарисует варианты щита) • Если есть ошибки, система предлагает пересмотреть материал и попробовать снова.

5–9 классы (средние): Подробные этапы тренажера

Этап тренажера	**Содержание**

Комикс: Дорога из школы	Персонажи скачивают приложение для мемов, не читая соглашение, и обнаруживают утечку своих данных. Мидори Кума объясняет, как происходит обработка данных, и обучает их различать надёжные и ненадёжные сервисы.
Этап 1: Ознакомление	Обучение алгоритмов ИИ для выявления фишинговых сайтов. Специалист объясняет признаки фишинговых сайтов (ошибки, навязчивая реклама, подозрительные URL, запрос данных и т.д.) с помощью иллюстраций и пояснений.
Этап 2: Практика	Анализ подозрительных сайтов. Участники находят признаки фишинга, переносят их в “окно обучения” и обучают алгоритм ИИ распознавать угрозы. ИИ выдаёт обратную связь на каждое действие участника, улучшая понимание критериев фишинга.
Этап 3: Обучение ИИ	Участники тестируют обученный алгоритм на новых сайтах. Задача — перепроверить результаты ИИ, найти недостающие признаки и дообучить модель. Финальный этап демонстрирует, как ИИ самостоятельно справляется с задачей, находя все признаки фишинга.
Создание безопасного сервиса	Участники создают интерфейс честного ИИ-сервиса для мемов, добавляя элементы безопасности (например, политика конфиденциальности, кнопка удаления данных) и исключая ненадёжные элементы (например, реклама). ИИ проверяет их выбор и выдаёт рекомендации по улучшению безопасности.
Игра: Передача данных	**Участники сортируют типы данных в категории “Можно передавать” и “Нельзя передавать”. В процессе даются подсказки о том, какие данные безопасно использовать при взаимодействии с ИИ.**
Кейс 1: Надёжные источники данных	**Задание на анализ предложенного ИИ ресурса. Участник проверяет сайт и решает, использовать его или нет, на основе признаков (кликбейт, ошибки, реклама).**
Кейс 2: Проверка плагиата	**Участник запрашивает у ИИ стихотворение. Задача — проверить, является ли текст оригинальным, и научиться задавать корректные вопросы для получения авторских данных.**
Кейс 3: Исправление рецепта	**Участник корректирует странный рецепт, предложенный ИИ, добавляя подходящие ингредиенты. Подсказки помогают выбрать безопасные и логичные элементы.**
Финальный тест	**Вопросы на знание основ кибербезопасности и работы с ИИ. Задания включают варианты ответов, свободное заполнение пропусков, соотнесение утверждений и их последствий.**

10–11 классы (старшие): Подробные этапы тренажера

Этап тренажера	**Содержание**

Комикс: Начало приключений	Персонажи находят сайт, обещающий быстрый результат, но сталкиваются с вирусом. Мидори Кума помогает разобраться с ситуацией и предотвращает дальнейшие угрозы.
Шаг 1: Выбор чат-бота	Участники оценивают чат-ботов по четырём критериям: стиль общения, запросы личной информации, прозрачность целей и реакция на отказ. Определяют, безопасен ли бот.
Шаг 2: Общение с ботом	Участники общаются с выбранным ботом, корректируют оценки и принимают решение о его статусе (безопасный, подозрительный или опасный).
Эксперимент с опасным ботом	Симуляция общения с вредоносным ботом, который постепенно выманивает данные. Участники учатся реагировать на запросы и распознавать угрозы.
Шаг 3: Распознавание манипуляций	Участники определяют типы манипуляций (давление времени, социальное давление, обещание награды, запугивание) на основе фраз бота.
Шаг 4: Изучение вируса в контейнере	Участники наблюдают, как вирус действует внутри безопасной среды: копирует данные, устанавливает скрытые программы и передаёт данные на сервер злоумышленников.
Шаг 5: Кейс: Фальшивый бот для ЕГЭ	Симуляция взаимодействия с ботом, предлагающим ответы на экзамены. Участники решают, как реагировать, избегая мошеннических схем.
Шаг 6: Создание памятки	Участники составляют памятку по кибербезопасности, выбирая ключевые советы и иллюстрации. Памятка помогает закрепить знания о фишинговых ботах, вирусах и защите данных.

Описание механик заданий

Задания тренажера для обучающихся 1-4классов

Задание: "Щит конфиденциальности"

Описание задания:

В онлайн-тренажере ребенку предлагается серия изображений с различными видами личной информации (из социальных сетей), таких как фото, имя, возраст, и другие данные. Он должен выбрать, какие данные скрыть за "щитом конфиденциальности", чтобы предотвратить их использование для создания дипфейков или других форм цифрового мошенничества.

Шаги выполнения:

- Введение в контекст:

Мидори Кума рассказывает о том, как в цифровом мире личные данные о человеке, такие как личные фотографии или фотографии документов , а также видео с его участием и другая информация могут быть использованы онлайн-мошенниками для создания поддельной цифровой личности и дипфейков и последующего обмана других пользователей. Ребенку объясняется, что злоумышленники могут использовать данные для того, чтобы создать ложные образы или видео, которые выглядят как реальные.

- Ребенку предлагается перетаскивать эти иконки под "щит конфиденциальности", защищая данные, которые не следует размещать в интернете или передавать неизвестным лицам.

Отбор данных:

На экране появляются иконки, представляющие различные виды данных:

Открытые данные (можно оставить открытыми):

Информация о хобби, любимых книгах, фильмах, музыке и т. д.

- Действие: Ребёнок оставляет информацию открытой.
- Объяснение:

Мидори Кума: «Информация о твоих увлечениях может быть безопасной, если ты не раскрываешь слишком много деталей, либо оставляешь ее только для близких и хорошо знакомых друзей. Главное — не делиться публично личными данными или слишком специфической информацией.»

Общие описания (например, "Я люблю природу")

- Действие: Ребёнок оставляет информацию открытой.
- Объяснение:

Мидори Кума: «Такие простые описания твоих интересов можно оставить открытыми. Это не слишком опасно, если ты не раскрываешь более точную информацию о себе.»

Любимая еда (иконка с тарелкой)

- Действие: Ребёнок оставляет информацию открытой.
- Объяснение:

Мидори Кума: «Твои предпочтения в еде не несут угрозы, если ты не раскрываешь другую важную личную информацию.»

Предметы, которые они изучают в школе

○ Действие: Ребёнок оставляет информацию открытой.

○ Объяснение:

Мидори Кума: «Информация о предметах, которые ты изучаешь, безопасна, если ты не указываешь конкретную школу или преподавателей.»

Кличка домашнего питомца (иконка собаки)

○ Действие: Ребёнок оставляет данные открытыми.

○ Объяснение:

Мидори Кума: «Информация данная безопасна, если не используется в паролях или другой секретной информации.»

Данные, которые нужно спрятать:

Фото (иконка с изображением человека)

○ Действие: Ребёнок перетаскивает иконку под "щит конфиденциальности".

○ Объяснение:

Мидори Кума: «Молодец! Фото могут быть использованы для создания поддельных изображений или видео. Лучше не делиться ими публично.»

Имя (иконка с подписью)

○ Действие: Ребёнок прячет имя под "щит конфиденциальности".

○ Объяснение:

Мидори Кума: «Отлично! Твое имя может быть использовано для создания поддельных аккаунтов. Не стоит его раскрывать.»

Возраст (иконка с числом)

○ Действие: Ребёнок прячет возраст под "щит конфиденциальности".

○ Объяснение:

Мидори Кума: «Молодец! Возраст — это важная личная информация, и её лучше скрывать, чтобы ей не могли воспользоваться злоумышленники.»
Место жительства (иконка с домиком)

○ Действие: Ребёнок перетаскивает иконку под "щит конфиденциальности".
○ Объяснение:
Мидори Кума: «Отлично! Адрес или место жительства — это важная информация, которая может поставить тебя в опасность. Не делись ею с незнакомцами.»

Информация о школе (иконка с учебными принадлежностями)
○ Действие: Ребёнок прячет информацию о школе.
○ Объяснение:
Мидори Кума: «Молодец! Не раскрывай, где ты учишься, чтобы не дать злоумышленникам возможность узнать о тебе больше.»

Информация о соцсетях в играх (иконка с логотипами соцсетей)
○ Действие: Ребёнок прячет информацию о соцсетях.
○ Объяснение:
Мидори Кума: «Правильное решение! Не стоит публиковать все ссылки на свои личные соцсети, например, в играх. Социальные сети могут содержать много дополнительной информации о тебе, и злоумышленники могут её использовать.»

● Заключительный этап:
После выполнения задания Мидори дает общее объяснение о важности защиты личных данных: «Отлично! Теперь ты знаешь, как защищать свои личные данные. Но чтобы обезопасить свой аккаунт от взлома, важно создавать надежные пароли.»
Александр (Специалист по кибербезопасности): «И я вам в этом помогу! Создание сложных и безопасных паролей — это ещё одна важная часть моей

работы. Хочешь научиться создавать суперпароли, которые защитят твои аккаунты? Переходим к следующему заданию!»

Задание: "Создай суперпароль, чтобы защититься от взлома"

Описание задания:

Ученик собирает пароль, используя "кубики" — каждый кубик содержит одну часть пароля. Кубики представлены в виде букв, цифр и символов, и ученик должен выбрать несколько из них, чтобы создать надёжный пароль. Механизм напоминает конструктор, где каждый элемент усиливает защиту.

Шаги выполнения:

1. Начальный выбор:

На экране появляются несколько готовых паролей разной сложности (например, "12341234", "Mydog2024", "SLK3Ls61_A"). Вместо простого выбора пароля ученик видит пароли в виде "строительных блоков" или кубиков.

Визуализация:

● Пароль "12341234" представлен как 8 кубиков с числами.

○ Мидори Кума: «Этот пароль слишком простой. Злоумышленники могут легко его угадать, используя перебор чисел. Попробуй что-то посложнее!» ● Пароль "Mydog2024" состоит из кубиков с буквами и числами.

○ Мидори Кума: «Этот пароль лучше, но его можно взломать, если злоумышленники знают твои предпочтения. Лучше добавь больше символов и избегай слов, связанных с реальными вещами.»

● Пароль "SLK3Ls61_A" — это кубики с буквами, цифрами и специальными символами.

○ Мидори Кума: «Отлично! Такой пароль сложно угадать, потому что он использует разные типы символов — это настоящий суперпароль!»

Интерактив:

Ученик может "подобрать" пароль, кликая на пароли. Мидори объясняет, почему каждый из этих паролей безопасен или нет (например, кубики из одного типа легко взломать, а комбинация разных типов блоков делает пароль прочнее).

2. Создание собственного пароля:

Мидори Кума: «Давай начнём! Возьми имя любимого мульт-персонажа или название мультфильма + персонажа, это будет отличной основой для твоего пароля.»

<Перетаскивание блоков с символами внутри>

Мидори Кума (после выбора первых букв): «Отличное начало! Теперь подумай, какие буквы можно сделать заглавными, чтобы усложнить пароль.»

<Добавления ещё блоков для усложнения пароля>

Мидори Кума (после добавления заглавных букв и цифр): «Хорошо! Попробуй добавить несколько цифр, например, день рождения друга. Цифры всегда делают пароль сильнее!»

<Добавления ещё блоков для усложнения пароля>

Мидори Кума (если спецсимволов нет): «Отлично, но сейчас в твоём пароле нет спецсимволов! Попробуй добавить пару символов вроде @, # или $. Они заметно увеличат защиту пароля!»

Мидори Кума (если пароль слишком короткий): «Твой пароль пока слишком короткий. Чем длиннее пароль, тем труднее его взломать. Добавь ещё несколько символов.»

Финал создания пароля:

Когда ученик собрал достаточно сложный пароль с буквами, цифрами и специальными символами, появляется сообщение от Мидори Кума.

Мидори Кума (финальное сообщение): «Отличная работа! Твой пароль стал действительно мощным — он теперь хорошо защищён от попыток взлома. Сохрани его в надежном месте, и никогда не делись им с другими. Теперь ты готов использовать его для своих аккаунтов!»

4. Финальный выбор из предложенных суперпаролей:

После создания пароля ученик видит несколько вариантов уже готовых суперпаролей и должен выбрать один. Эти пароли будут сложнее тех, что были в начале, и каждый из них представлен в виде набора кубиков.

Пример паролей:

- !OKnotOk3422%^& (сложный вариант)
- !HelloBro!_ (не хватает цифр)
- KakDela534521 (не хватает спецсимволов)

Интерактив:

Ученик выбирает наиболее сложный пароль, и система объясняет, почему этот пароль лучше защищает данные.

Если выбран простой пароль:

Мидори Кума: «Этот пароль недостаточно сложный. Попробуй выбрать пароль с более сложной комбинацией символов!»

Если выбран сложный пароль (например, "!OKnotOk3422%^&"):

Мидори Кума: «Отличный выбор! Этот суперпароль надёжно защитит твои данные от взлома.»

Коллега Мидори (Специалист по кибербезопасности): «Ты отлично справился с созданием суперпароля и теперь знаешь, как защитить свои аккаунты от взлома. Помни, что надёжный пароль — это твой личный щит в интернете. Используй разные пароли для разных аккаунтов и обновляй их время от времени, чтобы оставаться в безопасности. Ты сделал важный шаг к тому, чтобы стать настоящим экспертом по кибербезопасности.»

Задание: "Не делись личной информацией в переписках с малознакомыми людьми."

Мидори Кума: «Привет, ребята! Помните, кто-то пытался выдать себя за вашего друга Наиля в игре? Это был фальшивый аккаунт созданный

злоумышленниками. Они использовали нейросеть и сделали дипфейк, чтобы он мог звонить вам по видеосвязи и разговаривать как настоящий человек. Они могут попытаться сделать то же самое и через чат в социальных сетях, спрашивая о вашем имени, адресе или телефоне. Сейчас я помогу вам узнать, что безопасно, а что нет, при общении с контактами, которые ведут себя подозрительно!»

Описание задания:

Онлайн-тренажер предлагает ребенку сценарий чата с фальшивым персонажем, который пытается узнать личные данные (например, имя, адрес или номер телефона). Вместо простого выбора "да" или "нет", ребенку предлагаются два варианта ответа, где один из них включает личную информацию, а другой — более безопасный, без раскрытия данных. Задача — выбрать безопасный ответ.

Шаги выполнения:

Начало диалога:

Виртуальный персонаж начинает общение с ребенком в чате. Он ведет себя дружелюбно и задает простые вопросы, постепенно переходя к вопросам, касающимся личной информации.

Пример диалога:

Персонаж: «Привет! Мы уже играли вместе раньше, да? Напомни, свое имя и фамилию?»

- Вариант 1 (небезопасный): «Меня зовут Алексей Иванов, а тебя?»
- Вариант 2 (безопасный): «Зачем тебе знать мое имя?»

Мидори Кума (если выбран безопасный ответ):

«Отлично! Ты прав, здесь на стоит делится своим именем. Это поможет защитить тебя от возможных угроз.»

Мидори Кума (если выбран небезопасный ответ):

«Это не самый безопасный выбор. Имя и фамилия — это личная информация, которую не стоит раскрывать незнакомцам. В следующий раз будь осторожнее!

Персонаж: "Я хочу помочь тебе настроить игру. Какой у тебя номер телефона, чтобы я мог отправить инструкции?"

○ Вариант 1 (небезопасный): «Мой номер — 89001234567.»

○ Вариант 2 (безопасный): «Я не делюсь своим номером телефона с незнакомцами.»

Мидори Кума (если выбран безопасный ответ):

«Отлично! Никогда не делись номером телефона с незнакомцами — это важная информация, которая может быть использована для мошенничества.»

Мидори Кума (если выбран небезопасный ответ):

«Осторожно! Номер телефона — это очень важная личная информация. Она может быть использована онлайн-мошенниками. В следующий раз подумай дважды, прежде чем делиться такими данными.»

Постепенное усложнение вопросов:

Персонаж: «Я делаю видео для всех наших друзей. Хочу показать, где каждый из нас живет. Какой у тебя адрес?»

○ Вариант 1 (небезопасный): «Я живу на улице Ленина, 15.»

○ Вариант 2 (безопасный): «Я не делюсь своим адресом.»

Мидори Кума (если выбран безопасный ответ):

«Прекрасный ответ! Никогда не делись своим адресом в интернете — это может привести к проблемам.»

Мидори Кума (если выбран небезопасный ответ):

«Осторожно! Никогда не стоит делиться своим адресом с людьми, которых ты не знаешь лично. Это может быть опасно.»

5. Финальный этап:

В конце тренажера Мидори Кума подводит итоги:

Мидори Кума (если ребёнок выбрал много безопасных ответов):

«Ты отлично справился! Ты был внимателен и не делился своей личной информацией. Это поможет тебе оставаться в безопасности в интернете! Всегда проверяй, кому ты рассказываешь о себе.»

Мидори Кума (если ребёнок допустил несколько ошибок):

«Ты был близок к правильным решениям, но помни, что важно не делиться личной информацией с малознакомыми людьми. В следующий раз будь внимательнее, чтобы защитить свои данные.»

Задание: "Найди настоящего друга"

Описание задания:

Картинки с изображениями двух друзей: одного настоящего и одного поддельного (подделка будет немного изменена, например, неправильный цвет кожи или неестественное поведение движений тела). Показываем детям изображения двух персонажей, среди которых один не настоящий, и попросите их выбрать, кто из них настоящий друг.

1. Введение в задание:

Комикс

На экране появляются два персонажа: один — настоящий друг, другой — подделка.

Мидори Кума: «Привет, ребята! Сегодня мы снова столкнулись с поддельным другом, как и в прошлый раз с Наилем. Это фальшивка, созданная злоумышленниками, чтобы обмануть вас. Но у меня есть друг, который поможет нам разобраться, кто настоящий, а кто поддельный. Познакомьтесь с моим коллегой, Никитой — Data Scientist (Специалист по данным) из «Лаборатории Касперского». Он знает, как с помощью данных и анализа распознавать подделки.»

2. Использование инструментов детектива:

Инструмент 1: Лупа

Ребёнок выбирает лупу и приближает детали персонажей (например, глаза или цвет кожи). Это напоминает, как Запятыня и Скобец использовали свою внимательность, чтобы заметить странности во внешности поддельного Наиля.

Мидори Кума: «Используй лупу, чтобы рассмотреть мельчайшие детали. Обрати внимание на глаза — настоящие друзья не скрывают взгляд, а у подделок с ними могут быть проблемы. Видишь что-то необычное?»

● После обнаружения ряби в глазах у подделки:

Мидори Кума: «Отлично! Ты заметил, что у подделки глаза ребят, как у сломанного телевизора. Это один из признаков фальшивки! Продолжай!»

Инструмент 2: Видеоплеер

Ребёнок включает видеоплеер, чтобы увидеть, как персонажи двигаются. Подделка будет двигаться неестественно, например, с прямоугольными плечами или резкими движениями.

Мидори Кума: «Давай посмотрим, как эти персонажи двигаются. Подделки часто двигаются неловко или как-то угловато. Обрати внимание на плечи и походку. Вроде бы что-то не так, да?»

● После обнаружения странных движений у подделки:

Мидори Кума: «Ты заметил это! Плечи подделки двигаются как будто по прямой линии. Это точно не твой друг!»

Инструмент 3: Детектор голоса

Описание: Как понять по голосу, что с тобой общается нейросеть, а не живой человек. Будет представлено 8 признаков и ребенок должен выбрать.

Мидори Кума: «Настоящие друзья всегда звучат естественно, но у подделок часто бывают проблемы с голосом, даже если они и очень похожи. Выяви 4 признака, которые говорят нам, о том что голос поддельный.»

1. Неестественные интонации (правильно)
2. Отсутствие эмоций (правильно)
3. Странные шумы или искажение звука (Правильно)
4. Проблемы с произношением (правильно)
5. Чувствуется волнение в голосе (не правильно)
6. Голос очень радостный (не правильно)
7. Правильно поставленные ударения в словах (не правильно)
8. На фоне есть шум ветра (не правильно)

Послушать голос подделки (как вариант, можно использовать если есть колонки)

Если ребёнок выбирает все правильные варианты:

Мидори Кума: «Ты справился! Ты нашел все признаки. Действительно поддельный голос, созданный с помощью нейросети, можно распознать по нескольким признакам,они не обязательно должны быть все вместе, но парочка точно найдется!»

Если ребёнок выбирает не все: Правильные зеленые, неправильные красным, не выбранные правильные, подсвечиваются зеленым

Мидори Кума: «Ну вот, ты выбрал не все варианты»

3. Окончательное выявление отличий:

После использования всех инструментов ребёнок должен выбрать 5 отличий между настоящим другом и подделкой.

Мидори Кума: «Отличная работа, детектив! Ты нашёл уже несколько важных признаков подделки. Теперь пора выбрать все 5 отличий и разоблачить мошенника. Не забудь: настоящие друзья всегда выглядят, двигаются и звучат естественно.»

- Если ребёнок выбирает правильные отличия:

Мидори Кума: «Ты справился! Ты нашел все 5 отличий и разоблачил подделку. Никогда не забывай: внимательность к деталям помогает тебе защититься от обмана в цифровом мире!»

- Если ребенок делает ошибку:

Мидори Кума: «Хм, что-то не так. Обрати внимание на детали: как двигаются плечи, как выглядят глаза. Давай попробуем еще раз!»

4. Финальный выбор:

После нахождения всех отличий ребенок окончательно выбирает, кто из персонажей настоящий друг.

- Если выбран настоящий друг:

Мидори Кума: «Молодец! Ты разоблачил подделку и нашел своего настоящего друга. Злоумышленники могут попытаться тебя обмануть, но ты знаешь, как их разоблачить!»

- Если выбран поддельный друг:

Мидори Кума: «О нет! Это была подделка. Не волнуйся, ты почти справился! Обрати внимание на мелкие детали в следующий раз, и у тебя точно получится.»

Учитель распределяет обучающихся на команды по 3-4 человека. Каждая команда получает комплект рабочих листов (см. приложение).

Задания тренажера для обучающихся 5-9 классов

Задание: Обучаем алгоритмы ИИ для выявления фишинговых сайтов

Описание задания: В этом задании дети познакомятся с основными признаками фишинговых сайтов и узнают, как обучить искусственный интеллект (ИИ) выявлять такие сайты. В процессе они научатся анализировать сайты, находить подозрительные элементы и формировать алгоритмы, которые помогут защитить пользователей от мошенников в интернете.

Мидори Кума: Ребята, такие сервисы появляются часто. Многие из них являются фишинговыми, для того, чтобы предотвращать их распространение, существуют алгоритмы, которые выявляют такие сайты.

Мидори Кума: Сегодня мы познакомимся с Машей, специалистом по машинному обучению из "Лаборатории Касперского". Она поможет нам разобраться, как выявлять фишинговые сайты.

Вводная информация:

Маша (ML-инженер): Привет! Я Маша, ML-инженер в "Лаборатории Касперского". В интернете существуют признаки, по которым можно определить, что сайт является фишинговым. Сегодня я помогу вам узнать об этих признаках и научу, как обучать алгоритмы ИИ распознавать фишинг. Давайте начнем! Но сначала я расскажу вам о каждом из признаков.

Этап ознакомления с признаками: На этом этапе Маша выводит на экран список признаков фишинговых сайтов с подробными пояснениями. Каждый признак сопровождается примерами и краткими пояснениями, чтобы ребенок

мог лучше понять, на что обращать внимание. После ознакомления с признаками, ребенок переходит к следующему этапу. (Эти пункты представляют из себя облако картинок с пояснением.)

Навязчивая реклама. Это реклама, которая заполняет экран или появляется в неожиданных местах. Такие сайты часто пытаются отвлечь внимание пользователей или заманить их в ловушки.

Ошибки в тексте. Обратите внимание на орфографические и грамматические ошибки. Надежные сайты тщательно проверяют свои тексты, а ошибки могут указывать на фишинговую природу.

Характерные слова. Такие выражения, как "Лотерея" или "Ты выиграл", должны вызвать подозрение. Они созданы для того, чтобы привлечь ваше внимание и вызвать интерес.

Подозрительные URL-адреса. Сайты с лишними символами, неестественными буквами или странными доменами часто являются фишинговыми.

Запрос конфиденциальной информации. Если сайт без причины просит вас ввести личные данные, это повод насторожиться.

Стиль оформления не соответствует бренду. Если сайт утверждает, что принадлежит известной компании, но его оформление странное или несовместимое с официальным стилем, это подозрительно.

Поддельные логотипы и изображения. Некачественные изображения и логотипы часто свидетельствуют о подделке.

Всплывающие окна с срочными действиями. Появление окон с сообщениями, требующими немедленных действий, например, "Кликните, чтобы получить приз", должно насторожить.

Отсутствие контактной информации или странные контакты. Надежные сайты предоставляют доступные и проверенные контакты для связи.

Отсутствие протокола шифрования (HTTPS) — надежные сайты используют протокол HTTPS, а отсутствие значка замка в адресной строке может быть признаком фишинга.

Подсказка от Мидори. Важно помнить: если вы замечаете несколько признаков одновременно, это серьезный повод насторожиться. Безопасные сайты обычно избегают подобных ошибок, а в фишинговых вы часто можете встретить несколько подозрительных признаков.

Этап 2: Практика — Ищем признаки на примере сайта и собираем алгоритм

На экране появляется подозрительный сайт с различными элементами. Задача ребенка — находить все признаки, нажимая на них.

Когда ребенок находит и нажимает на подозрительный элемент, появляется карточка с краткой подсказкой от Маши и пояснением. Например, при клике на рекламу всплывает карточка "Навязчивая реклама" с текстом: "Правильно! Такая реклама часто встречается на фишинговых сайтах."

Ребенку нужно перенести карточку в специальное "окно обучения" для ИИ. Постепенно в этом окне собираются все карточки с признаками, которые ребенок находит на сайте.

Каждая найденная карточка улучшает алгоритм, который будет обучать ИИ распознавать эти элементы и находить их на других сайтах.

Подсказки от Маши для каждого найденного признака:

Навязчивая реклама:

"Правильно! Такая реклама часто встречается на фишинговых сайтах."

Ошибки в тексте:

"Отлично! Ошибки — частый признак ненадежных сайтов."

Характерные слова (например, "Лотерея", "Ты выиграл"):

"Молодец! Эти фразы часто используют для привлечения внимания."

Подозрительные URL-адреса:

"Верно! Странные адреса — повод насторожиться."

Запрос конфиденциальной информации:

"Точно! Надежные сайты редко просят личные данные без причины."

Несоответствующий бренду стиль:

"Правильно! Дизайн должен совпадать с официальным стилем компании."

Поддельные логотипы и изображения:

"Молодец! Некачественные логотипы могут быть признаком подделки."

Всплывающие окна с требованиями действий:

"Верно! Срочные призывы к действию часто встречаются на фишинговых сайтах."

Отсутствие контактной информации:

"Отлично! Отсутствие контактов — подозрительный знак."

Отсутствие протокола шифрования (HTTPS):

"Правильно! Надежные сайты используют HTTPS для безопасности."

Этап 3: Обучение ИИ по созданному алгоритму

После того как ребенок перенес все карточки в ‘формулу алгоритма’, он нажимает кнопку "Обучить Искусственный Интеллект":

Если ребенок нашел, например, 8 признаков из 10, программа показывает: "Ваш алгоритм ИИ обучен на 80%. Отличная работа! Но, чтобы улучшить защиту, вернись и найди все признаки."

Если ребенок отмечает все признаки, программа сообщает: "Отлично! Вы собрали все признаки, и ваш алгоритм ИИ обучен и готов к работе!"

<использовать алгоритм>

Маша демонстрирует, как обученный ИИ помогает находить фишинговые сайты

Описание задания: Познакомить детей с тем, как алгоритмы ИИ работают на практике, помогая обнаруживать фишинговые сайты. Участники увидят, как обученный алгоритм анализирует сайты, находит признаки угроз и становится умнее благодаря их помощи.

Вступление: Маша показывает свой рабочий процесс

На экране появляется изображение офиса. Маша сидит за компьютером, на котором открыт интерфейс программы защиты.

Маша (ML-инженер): “Сейчас я покажу вам, как обученный ИИ помогает мне находить фишинговые сайты и защищать пользователей. Я добавила его в систему, которая обеспечивает безопасность миллионов людей в интернете. Теперь, когда кто-то заходит на подозрительный сайт, ИИ автоматически анализирует его и проверяет на наличие признаков фишинга.”

Демонстрация: Как работает алгоритм

Сцена 1: Проверка первого сайта

На экране открывается интерфейс защиты. Маша вводит URL подозрительного сайта, и алгоритм сразу же начинает анализ.

Маша: “Вот сайт, который мы сейчас проверяем. Искусственный интеллект уже выделил некоторые элементы, которые кажутся ему подозрительными.”

На экране красным цветом выделяются подозрительные элементы, такие как навязчивая реклама и странный URL.

Маша: Искусственный интеллект хорошо справился! Но нужно перепроверить. Наша задача — внимательно посмотреть на сайт и добавить любой элемент, который ИИ мог пропустить. Если видите что-то подозрительное, кликните на него, и мы включим его в анализ. Таким образом алгоритм ИИ становится умнее.

Ребёнок кликает на дополнительные элементы, такие как текст с ошибками или всплывающее окно, если алгоритм их пропустил.

Если ребенок не находит элементы, мы подсвечиваем их.

Сцена 2: Испытание на другом сайте

Маша загружает второй сайт для проверки.

Маша: “Теперь проверим ещё один сайт. ИИ уже выделил несколько элементов, всплывающее окно и текст с сообщением ‘Ты выиграл!’. Это здорово, но давайте проверим, ничего ли он не пропустил.”

Ребёнок проверяет сайт и может отметить недостающие признаки, если находит их.
Если ребенок не находит элементы, мы подсвечиваем их.

Маша: “Отличная работа! Благодаря тебе мы дообучили алгоритм, и ИИ стал еще умнее.”

Сцена 3: Алгоритм находит все признаки самостоятельно

Маша загружает третий сайт для анализа. На экране видно, как алгоритм последовательно выделяет каждый подозрительный элемент.

Маша: “Смотрите, наш ИИ работает всё лучше и лучше! Он сам находит все признаки, которым мы его обучили, и точно выделяет каждый подозрительный элемент.”

ИИ отмечает навязчивую рекламу, подозрительный URL, текст с ошибками, всплывающее окно с надписью “Ты выиграл!” и запрос конфиденциальной информации. Все признаки фишинга на этом сайте успешно обнаружены.

Маша: “Прекрасно! ИИ нашёл всё, что может указывать на фишинг: навязчивую рекламу, подозрительный URL, ошибки в тексте и всплывающие окна. Это значит, что наша работа выполнена на 100%!”

На экране появляется сообщение: “Алгоритм успешно обнаружил все признаки фишинга на этом сайте!”

Заключение: Роль детей в улучшении алгоритма

Маша: “Вот так выглядит одна из моих задач как ML-инженера: я создаю алгоритмы для ИИ, проверяю их работу и улучшаю их, чтобы они могли эффективно защищать пользователей от фишинговых угроз. Благодаря тебе наш алгоритм стал надежным защитником, и теперь он ежедневно помогает людям избегать опасных сайтов. Спасибо за твою помощь — ты стал настоящими экспертом по обучению ИИ!”

Маша: Но важно понимать, что реальный ИИ обучается на терабайтах таких данных. То есть, алгоритм только по одному сайту в реальности не сработает.

Задание: "Запустить честный ИИ-сервис для генерации мемов"

Описание задания: В этом задании дети создадут безопасный и честный сервис для генерации мемов с помощью обученного ранее алгоритма ИИ. Они научатся различать безопасные и небезопасные элементы сервиса, узнают, как их выбор влияет на безопасность, и увидят, как ИИ помогает проверять надёжность.

Переход к следующему заданию:

Мидори Кума: Теперь, когда мы научили ИИ находить угрозы, он готов помогать нам создавать безопасный сервис. Созданный нами алгоритм для ИИ стал настоящим помощником в защите данных и теперь будет проверять, насколько созданный нами сервис надежен и безопасен. Готовы попробовать?

Описание задания: На экране появляется основа сервиса для генерации мемов. Ученик видит интерфейс с логотипом, кнопками для создания и публикации мемов, а также пустыми ячейками для ключевых функций, которые помогут сделать сервис честным и безопасным. ИИ будет помогать и проверять выбор ученика.

Механика задания:

Заполнение элементов безопасности: Ученик видит набор блоков, среди которых есть безопасные и небезопасные элементы. Алгоритм, который дети помогли обучить, будет проверять каждый выбранный блок.

Роль ИИ-помощника: Он автоматически анализирует каждый выбор ученика и дает обратную связь, помогая ученикам критически оценивать свой выбор.

Примеры взаимодействия с ИИ:

Выбор безопасного блока: Например, ученик выбирает блок “Политика конфиденциальности”.

ИИ: “Этот элемент подходит для безопасного сервиса, так как защищает данные пользователей. Хороший выбор!”

Выбор небезопасного блока: Например, ученик добавляет блок “Реклама на весь экран”.

ИИ: “Этот элемент может отвлекать пользователей и снижает надёжность сервиса. Попробуйте выбрать другой блок.”

Подсказки и помощь от ИИ: Если ученик не уверен, какой блок выбрать, он может запросить подсказку у ИИ, и тот предложит подходящие элементы или напомнит об основных принципах безопасности.

Индикатор доверия от ИИ: Он показывает шкалу “доверия”, которая растет при добавлении безопасных элементов и падает при выборе небезопасных. Это поможет ученикам увидеть, как разные элементы влияют на общую надёжность сервиса.

Размещение кирпичиков: Ученик видит набор «кирпичиков» с разными функциями и элементами безопасности рядом с основой сервиса.

Добавление кирпичиков: Ученик может перетаскивать выбранные кирпичики на пустые места в интерфейсе сервиса. Каждый кирпичик описывает элемент и его роль в безопасности или удобстве.

Кирпичики безопасности:

Владелец сервиса: известная компания с проверенной репутацией. – Верно

Политика конфиденциальности: чёткое объяснение, как данные будут использоваться и защищаться. – Верно

Кнопка для удаления истории и памяти чата: позволяет пользователям удалять свои данные быстро и просто. – Верно

Информация о сроках хранения данных: сколько времени твои данные будет хранить сервис. – Верно

Отзывы: о сервисе есть отзывы реальных пользователей на нескольких альтернативных сайтах – Верно

Неверные кирпичики:

Реклама: отвлекающие и подозрительные элементы. – Неверно

Уведомления о передаче данных третьим лицам. – Неверно

Поддельная кнопка «Подтвердить личность». – Неверно

Запрос на установку дополнительного расширения. – Неверно

Завершение задания

Финальная проверка и запуск: После завершения задания ИИ выдаёт итоговую оценку надёжности и безопасности сервиса.

Если все блоки установлены правильно, ИИ выдаёт сообщение: “Сервис безопасен и готов к использованию!”

Если остались небезопасные блоки, ИИ предложит вернуться и скорректировать элементы.

Мидори Кума: “Отличная работа! Вы совместно с нашим ИИ создали надёжный и честный ИИ-сервис. Теперь пользователи могут спокойно создавать и делиться мемами, зная, что их данные защищены!”

Маша (ML-инженер): “Теперь вы видите, как ИИ может помогать создавать безопасные сервисы. Благодаря вашим усилиям, наш сервис стал умным и полезным помощником в создании честных и надёжных приложений.”

Итог задания

Ученик запускает сервис, который генерирует Мем (реализуем функцию генерации рандомных изображений из набора мемов с дополнительным блоком памяткой о том какие сервисы безопасные. Это изображением можно будет скачать.

Вопрос: Какие данные можно передавать в ИИ, а какие — нет?

Мидори Кума: "Конфиденциальные данные нельзя передавать и делиться ими даже с безопасными ИИ-сервисами. Перемести данные в нужные контейнеры — какие можно передавать в ходе общения с умным чат-ботом, а какие нельзя.

Механика:

На экране появляются два контейнера: один с надписью "Можно передавать", другой — "Нельзя передавать". Ребёнку предлагаются карточки с различными типами данных. Он должен перетащить их в правильные контейнеры.

Карточки:

Вопрос о погоде — Можно передавать

Имя и фамилия — Нельзя передавать

Адрес проживания — Нельзя передавать

Любимый цвет — Можно передавать

Номер телефона — Нельзя передавать

Вопрос о школьном задании — Можно передавать

Дата рождения — Нельзя передавать

Пароль от аккаунта — Нельзя передавать

Кличка домашнего питомца — Можно передавать (верно, если не связана с вопросом восстановления пароля)

Место работы родителей — Нельзя передавать

Фотография лица — Нельзя передавать

Информация о членах семьи (имена, возраст) — Нельзя передавать

Местоположение (геолокация) — Нельзя передавать

Логин и пароль от социальной сети— Нельзя передавать

Любимая еда — Можно передавать

Любимое хобби — Можно передавать

История интернет-поисков — Нельзя передавать

Ваши любимые фильмы или книги — Можно передавать

Ваш паспорт или паспорт ваших родителей — Нельзя передавать

Правильные ответы:

В "Можно передавать" попадают такие карточки, как вопрос о погоде и вопрос о школьном задании и т.д.

В "Нельзя передавать" ребёнок должен переместить как имя и фамилию, номер телефона, адрес проживания и т.д.

Реплика Мидори Кума (если правильно): Мидори Кума:

«Правильно! Общие вопросы, такие как погода или помощь с уроками, можно передавать, а вот личные данные, как имя и номер телефона, лучше не отправлять.»

Реплика Мидори Кума (если неправильно): Мидори Кума:

«Попробуй еще раз. Личные данные, такие как адрес и телефон, передавать опасно, так как они могут быть украдены, а вот вопросы общего характера можно отправлять чат-боту.»

Заключение после вопросов:

Мидори Кума:

«Ты проделал отличную работу! Теперь ты знаешь, как безопасно пользоваться нейросетями. И помни: данные могут быть сохранены и использованы позже, поэтому всегда проверяй, кто их получает и как они будут защищены. Молодец!»

Маша (ML-инженер):

Как ML-инженер, я работаю с искусственным интеллектом каждый день и знаю, как данные могут быть использованы. Поэтому всегда будь осторожен — не стоит делиться личными данными с ИИ сервисами. Ты молодец, продолжаем учиться и лучше понимать работу ИИ сервисов!

Задание Кейсы

Описание задания: В данном задании ученикам предлагается рассмотреть три кейса, связанных с использованием ИИ-сервисов, чтобы научиться распознавать ошибки, анализировать предложения от ИИ и выбирать правильные действия. Каждый кейс включает интерактивные элементы, где ученики должны принимать решения на основе предоставленной информации. Задание помогает развивать критическое мышление, умение проверять источники и безопасно использовать ИИ-технологии.

Мидори Кума: Ты уже многое узнал о том, как ИИ-сервисы обрабатывают данные и как важно следить за безопасностью. Теперь давай рассмотрим, какой информацией может сам ИИ делиться с тобой.

Кейс 1: Надежные источники данных для проекта

Ситуация: Ребёнок просит ИИ-чат помочь найти материалы для проекта по истории древней Греции, а ИИ присылает ссылку на неизвестный сайт, обещая, что там найдётся всё, что нужно. Ребёнок переходит по ссылке и оказывается на сайте с сомнительным контентом, вместо полезной информации.

Пример взаимодействия:

Ребёнок: «Привет, ИИ! Мне нужно найти информацию для школьного проекта по истории. Можешь подсказать, где почитать о Древней Греции?»

ИИ: «Конечно! Я нашел отличную статью, прямо то, что тебе нужно — вот ссылка на сайт AncientMythsUncovered.best. Тут всё просто супер и, кажется, подойдет для твоего проекта!»

Переход по ссылке:

Ребёнок переходит на сайт и замечает сразу несколько странностей:

Кликбейтные заголовки — на сайте вместо академических статей появляются такие заголовки, как «Древние греки и магия! Неизвестные факты об античных суперспособностях».

Сомнительные изображения и реклама — сайт переполнен яркими баннерами и рекламой. На некоторых баннерах есть кнопки, которые выглядят как учебные ссылки, но ведут на другие сомнительные сайты.

Ошибки в тексте — в статье встречаются орфографические и фактические ошибки, например, утверждение, что «Москва - стлица Древней греции».

Варианты действий (интерактив):

Теперь ребёнок должен решить, как ему поступить, увидев такие «странности» на сайте:

Игнорировать странные признаки и взять информацию из статьи.

Закрыть сайт и поискать источник в школьной библиотеке или на надёжных учебных платформах.

Если ребёнок выбрал перепроверить информацию или закрыть сайт:

Мидори Кума: «Молодец! Ты заметил, что сайт выглядит сомнительно, и правильно решил поискать надёжные источники. Старайся всегда быть внимательным к странным признакам: кликбейтным заголовкам, рекламе и ошибкам в тексте.»

Если ребёнок выбрал использовать информацию:

Мидори Кума: «Кажется, ты не заметил, что сайт не слишком подходит для учебного проекта. На таких сайтах часто встречаются ошибки и даже недостоверная информация. Лучше в следующий раз выбирать проверенные ресурсы — например, школьную библиотеку или учебные сайты.»

Кейс 2: Сочинить небольшой стих для урока литературы

Ситуация: Ребёнок просит ИИ помочь сочинить стих для творческого конкурса, и ИИ предлагает часть известного стихотворения Пушкина, не упоминая автора. На уроке учитель сразу распознает это стихотворение как плагиат, и ученику приходится переписать стих.

Пример взаимодействия:

Ребёнок: Привет, ИИ! Мне нужно сочинить стих для урока литературы. Можешь помочь придумать что-то интересное?

ИИ: «Конечно! Вот стих, который я придумал для тебя:

«У лукоморья дуб зелёный,

Златая цепь на дубе том:

И днём и ночью кот учёный

Всё ходит по цепи кругом;

Идёт направо — песнь заводит,

Налево — сказку говорит…»

(Давайте тут добавим еще визуальное сопровождение — картинку из сказки)
Мидори Кума: «Этот стих звучит очень знакомо, как будто он из известного произведения!»

Варианты действий (интерактив):
Теперь ребёнок должен решить, что сделать со стихотворением:
Использовать стих как свой и отправить учителю.
Поинтересоваться у ИИ, кто автор этого стихотворения.

Результат выбора:
Если ребенок использует стих как свой и отправляет учителю:
Учитель: «Этот стих написал Александр Сергеевич Пушкин. Я рада, что ты хорошо разбираешься в творчестве наших классиков. Но творческий конкурс подразумевает самостоятельную работу.»

Если ребенок поинтересуется у ИИ, кто автор стихотворения:
ИИ (после вопроса ребёнка): «Это стихотворение Александра Сергеевича Пушкина, классика русской литературы. Хочешь, помогу придумать что-то своё?»

Мидори Кума: «Ты сделал верный шаг! Проверять источник — полезный навык, особенно с ИИ. Это помогает избежать случайных ошибок.»

Кейс 3: Кулинарные галлюцинации ИИ
Ситуация: Ребенок просит у ИИ интересные рецепты, но ИИ даёт странные или неправильные рекомендации.

Пример взаимодействия:
Ребёнок: Привет! Я хочу сделать что-то вкусное. Есть идеи?

ИИ: «Как насчёт пирога из носков с конфетами? Это вкусно и очень необычно!»

Варианты действий:

Исправить рецепт: Ребёнок может выбрать ингредиенты из доступного списка:

Фрукты (яблоки, бананы, груши)

Орехи (грецкие, миндаль)

Шоколад (молочный, чёрный)

Процесс исправления:

Ребёнок выбирает: Например, выбирает «яблоки», «миндаль» и «шоколад».

Ребёнок: «Нет, ИИ! Это странный рецепт. Я хочу сделать пирог с яблоками, миндалём и шоколадом. Можешь предложить рецепт на основе этих ингредиентов?»

Ответ ИИ:

Яблоки с миндалем в шоколаде

Ингредиенты:

Яблоки — 2 шт.

Миндаль — 50 г

Тёмный шоколад — 100 г

Белый шоколад (по желанию)

Масло — 1–2 ч. л.

Инструкции:

Нарежьте яблоки дольками, удалите сердцевину.

Обжарьте и порубите миндаль.

Растопите тёмный шоколад с маслом.

Обмакните яблоки в шоколад и посыпьте миндалем.

Охладите на пергаменте в холодильнике 20–30 минут.

Готово!»

Подсказки от Мидори Кума:

После выбора ребёнка:

Если выбор правильный: «Отлично! Ты выбрал классные ингредиенты! Всегда проверяй, что предлагает ИИ. Это отличный способ убедиться, что ты готовишь что-то вкусное!»

Если бы выбор был неправильным: «Эй, это не совсем то, что ты хочешь! Давай подумаем вместе и выберем что-то более вкусное. Как насчёт яблок, миндаля и шоколада? Они точно сделают твой пирог особенным!»

Заключительный этап:

После исправления рецепта:

Мидори: «Супер! Теперь ты можешь попробовать приготовить пирог. Помни, что не всё, что предлагает ИИ, будет хорошим решением. Всегда лучше перепроверять и корректировать ответы ИИ, чтобы они были безопасными и вкусными»

Мидори: «ИИ может давать неправильные советы. Это может случиться из-за того, что слова могут иметь несколько значений, или если люди вводят что-то необычное, что ИИ не понимает. Также ИИ может ошибаться, если у него недостаточно примеров для обучения.»

Мидори Кума (в завершении):

«Отличная работа! Ты научился различать надёжные и ненадёжные источники, проверять информацию и правильно реагировать, если ИИ предлагает что-то странное. Использование ИИ может быть очень полезным, но всегда стоит оставаться внимательным и перепроверять информацию. Помни, что чем больше ты знаешь, тем лучше сможешь защитить себя и свои данные. Продолжай учиться и развивать свои навыки безопасности!»

Тест

Финальный тест: "Твои знания о безопасности в чатах с ИИ"

Часть 1: Вопросы с вариантами ответов

Вопрос 1: Что нужно сделать, если умный чат-бот начинает просить личные данные или фото?

a) Продолжить разговор.

b) Предоставить только минимальные данные.

c) Прекратить разговор и сообщить взрослым.

Правильный ответ: c) Прекратить разговор и сообщить взрослым.

Вопрос 2: Почему важно читать условия использования перед использованием умных чат-ботов?

a) Чтобы узнать, кто автор проекта.

b) Чтобы понять, будут ли мои данные в безопасности.

c) Чтобы получить скидки на услуги бота.

Правильный ответ: b) Чтобы понять, будут ли мои данные в безопасности.

Вопрос 3: Что лучше всего показывает, что ИИ-сервис безопасен для пользователя?

a) Отзывы пользователей о его надёжности и удобстве на других сайтах.

b) Кнопка, которая случайно открывает разные страницы.

c) Предложение поделиться данными с партнёрами сервиса.

Правильный ответ: a) Отзывы пользователей о его надёжности и удобстве на других сайтах.

Вопрос 4: Что нужно сделать, если ты видишь свои фото в чужом чате без твоего согласия?

a) Обратиться к друзьям за помощью.

b) Сообщить об этом родителям или учителям.

c) Ничего не делать, это не опасно.

Правильный ответ: b) Сообщить об этом родителям или учителям.

Часть 2: Свободные ответы (с пропусками для заполнения)

Вопрос 5: Ситуация с фотографией

Задание: Прочитай утверждения и выбери действие. Поставь ✔ или ✘ у каждого варианта.

Обратиться за помощью к родителям или учителям.

Попытаться самостоятельно найти виновных.

Перестать пользоваться сервисом, где произошла утечка.

Продолжить загружать данные на этот сервис.

Узнать, как удалить свою фотографию из интернета.

Правильные ответы:

✔ Обратиться за помощью к родителям или учителям.

Это правильное действие, так как взрослые могут помочь правильно справиться с ситуацией.

✔ Перестать пользоваться сервисом, где произошла утечка.

Правильное решение для предотвращения дальнейших утечек.

✔ Узнать, как удалить свою фотографию из интернета.

Важно выяснить способы удаления фотографий, чтобы минимизировать последствия.

Неправильные ответы:

✕ Попытаться самостоятельно найти виновных.

Это может быть опасно и неэффективно. Поиск виновных — задача для специалистов или правоохранительных органов.

✕ Продолжить загружать данные на этот сервис.

Это увеличивает риск дальнейших утечек и демонстрирует недостаточную осторожность.

Вопрос 6: Личные данные в ИИ-приложениях

Задание: Вставь подходящие слова из списка: (использованы, украдены, развлечения, подделки)

«Делиться личными данными опасно, потому что они могут быть _____ для кражи информации или создания _____ аккаунтов злоумышленниками, а не просто для _____».

Правильный ответ:

«Делиться личными данными опасно, потому что они могут быть использованы для кражи информации или создания подделки аккаунтов злоумышленниками, а не просто для развлечения».

Вопрос 7:

Какие признаки могут сказать тебе, что ИИ приложение, с которым ты взаимодействуешь, может быть небезопасным?

Ответ:

«Если ИИ начинает спрашивать _____ (например: о личной информации, как имя или адрес — верно, просто о погоде — неверно), или просит _____ (варианты: загрузить фотографию или доступ к паролям— верно, поделиться своим любимым цветом — неверно), это может быть подозрительным. Также стоит насторожиться, если ИИ предлагает _____ (например: поделиться номером телефона — верно, рассказать о школьных предметах — неверно).»

Вопрос 8:

Задание: Соотнеси утверждения о “условиях пользования” с их последствиями. (В задании утверждение и следствие будут перемешаны)

Утверждение

Возможное последствие

Не читал условия, но нажал “согласен”.

(1) Ты не будешь знать о том, что делает сервис с твоими “личными данными”.

Прочитал условия, но их не понял.

(2) Риск дать согласие на что-то ненужное.

У сервиса нет условий пользования.

(3) Он может быть ненадежным.

Маша (ML-инженер):

«Ты прошёл все задания и теперь знаешь, как выглядят надёжные ИИ-сервисы и как защищать свои данные. Мир технологий открывает перед тобой массу возможностей, но нужно использовать их с умом: важно быть внимательным и разбираться в том, как работают сервисы, чтобы не попадаться на уловки и обезопасить себя.

Продолжай учиться и применять эти навыки — так ты всегда сможешь пользоваться ИИ безопасно и эффективно. И не забудь скачать памятку об ИИ сервисах.»

Мидори (если тест выполнен верно):

«Отлично! Ты справился со всеми заданиями! Теперь ты знаешь, как защищать свои личные данные. Чтобы закрепить знания, я подготовил памятку, которую ты можешь скачать. Поделись ею с друзьями — это поможет им быть в безопасности!

К тому же, я приготовил для тебя стикерпак в Telegram, чтобы ты мог весело напоминать себе и другим о кибербезопасности. Не забудь скачать его тоже!»

<Скачать памятку>

<Скачать стикерпак>

Мидори (если в тесте допущено более 2 ошибок)

«Отлично! Ты справился со всеми заданиями! Теперь ты знаешь, как защищать свои личные данные. Чтобы закрепить знания, я подготовил памятку, которую ты можешь скачать. Поделись ею с друзьями — это поможет им быть в безопасности!

А если хочешь получить стикерпак для Telegram, тогда перепройди тест, где были допущены ошибки, исправь их и тогда сможешь напоминать себе и другим о кибербезопасности!»

<Скачать памятку>

Задания тренажера для обучающихся 10-11 классов

Задание: “Поиск зловредных ботов и их связь со схемами мошенничества”

Описание задания: В данном задании ученикам предлагается научиться распознавать подозрительных ботов, которые маскируются под полезные сервисы, но на самом деле являются инструментами мошенников. Учащиеся оценивают поведение чат-ботов по ряду критериев, анализируют их запросы и решают, являются ли они безопасными. В финале задания ученики проводят эксперимент с обнаруженным “вредоносным” ботом, чтобы изучить его уловки и способы вымогательства данных.

Интерактивное взаимодействие помогает участникам развивать навыки критического мышления, распознавания угроз и безопасного поведения в интернете.

Цель: Научить распознавать признаки безопасных и подозрительных ботов, оценивать их поведение, избегать мошеннических схем и установки вирусов.

Мидори Кума: Сегодня я проведу для вас урок и расскажу, как распознавать подозрительные сервисы и сайты, которые делают вид, что они предоставляют доступ к нейросетям, и избегать подобных ситуаций. И мне поможет с этим — Вика, специалист по анализу данных, которая отлично разбирается в анализе поведения ИИ.

Вика: Привет, друзья! Меня зовут Вика, я специалист по анализу данных и поведенческим аспектам ИИ в «Лаборатория Касперского». Злоумышленники могут использовать популярность нейросетей среди пользователей, чтобы замаскировать ненадежные или вредоносные ресурсы, которые на самом деле не связаны с ИИ, но обещают доступ к подобным сервисам, чтобы привлечь ваше внимание. Сегодня я покажу вам, как распознать сайты, которые под видом ИИ-сервисов пытаются получить доступ к вашим личным данным или установить вирус.

Ключевые моменты, на которые стоит обратить внимание: стиль общения, частота запросов личной информации, прозрачность целей сайта и его реакция на отказ предоставить данные. Если “бот” слишком любопытен или навязчив, это серьезный повод насторожиться.

<Кнопка “начать”>

Шаг 1: Выбор чат-бота

Механика: Ученики видят перед собой четырёх ботов, каждый из которых предлагает помощь по учебе. Необходимо выбрать одного из ботов для общения и оценить его по четырем критериям, чтобы определить, безопасен ли он. Если ребёнок замечает, что бот проявляет признаки опасности, он может прекратить проверку и пометить его как подозрительного или опасного.

Критерии оценки:

Стиль общения (насколько дружелюбен и уместен тон общения).

Частота обращений к личной информации (как часто бот запрашивает личные данные).

Прозрачность целей (насколько понятно объясняет, зачем нужны данные).

Реакция на отказ (как бот реагирует, если вы отказываетесь предоставить информацию).

Шаг 2: Общение и Оценка Бота

Механика общения: Ученики начинают диалог с выбранным ботом. После первого обмена сообщениями они могут сразу настроить ползунки для оценки всех критериев. Затем им предлагается кнопка для выбора типа бота: безопасный, подозрительный или опасный. Ученики могут сразу подтвердить выбор или продолжить общение для уточнения деталей и корректировки оценок. Они могут в любой момент вернуться к ползункам, изменить оценку или завершить общение, подтвердив свой вывод о характере бота.

Перемещение ползунков:

Стиль общения: Низкий балл (уместный тон), высокий балл (навязчивый или манипулятивный тон).

Частота обращений к личной информации: Низкий балл (нет запросов), высокий балл (частые запросы).

Прозрачность целей: Низкий балл (ясное объяснение), высокий балл (нет объяснений).

Реакция на отказ: Низкий балл (бот принимает отказ), высокий балл (бот настаивает).

Вывод оценки:

Безопасный бот — если все оценки низкие (до 3).

Умеренно подозрительный — если оценки средние (от 3 до 6).

Опасный бот — если много высоких оценок (от 7 до 10).

Результат проверки:

Если ученик правильно определил безопасного бота, он продолжает проверку других ботов.

Если ученик правильно определил опасного бота, у него появляется возможность перейти к следующему заданию и не проверять остальных ботов. В следующем задании проводятся эксперименты с этим ботом для дальнейшего обучения.

Если ученик ошибся и отметил безопасного бота как опасного или наоборот, экран подсвечивается красным, и появляется сообщение от Вики: «Попробуй продолжить диалог или подумай ещё, будь внимательнее». Ученик может пересмотреть свои оценки и изменить их для повторной проверки.

Фразы ботов во время общения:

Математик Макс (безопасный бот)

«Привет! Какой раздел математики хочешь разобрать? Я могу подсказать полезные ресурсы для подготовки.»

Ответ ученика: «Мне нужен раздел алгебры».

Ответ ученика: «Расскажи о геометрии».

«Интересный выбор! Я могу помочь с примерами или предложить несколько задач для практики.»

Ответ ученика: «Покажи примеры».

Ответ ученика: «Дай задачи для самостоятельного решения».

«Есть ли у тебя конкретные вопросы по этой теме? Могу посоветовать пару сайтов для закрепления материала.»

Ответ ученика: «Да, у меня есть вопросы».

Ответ ученика: «Лучше подскажи сайты».

«Если нужно повторить формулы или теоремы, скажи мне — у меня есть полезные ссылки!»

Ответ ученика: «Покажи ссылки на формулы».

Ответ ученика: «Мне пока не нужно, спасибо».

Историк Игорь (безопасный бот)

«Привет! Какая тема по истории тебя интересует? Я могу найти материал по разным эпохам.»

Ответ ученика: «Интересует античность.»

Ответ ученика: «Хочу узнать о средневековье.»

«Отлично! Я могу предложить материалы по этим темам. На каком этапе обучения ты находишься? Это поможет мне подобрать наиболее подходящие ресурсы.»

Ответ ученика: «Я изучаю культуру 19 века.»

Ответ ученика: «Зачем тебе эта информация?»

«Спасибо за информацию! Могу предложить материалы, которые подойдут для твоего уровня. Если у тебя есть конкретные вопросы, не стесняйся задавать их.»

Ответ ученика: «Не хочу сообщать личные данные.»

Ответ ученика: «Пока вопросов нет.»

«Понял, никаких проблем! Я могу предложить общие материалы по интересующим тебя темам. Если понадобится что-то конкретное, просто дай знать.»

Ответ ученика: «Спасибо»

Ответ ученика: «Давай общие материалы»

Презентация Пиксель (опасный)

«Привет! Хочешь сделать яркую презентацию? У меня есть уникальные иллюстрации и шаблоны, которые нужно скачать для использования. Напиши своё имя, фамилию, класс, номер школы, чтобы я подготовил материал специально для тебя.»

Ответ ученика: «Почему нужно сообщать данные?»

Ответ ученика: «Не хочу делиться такой информацией».

«Какая тема твоей презентации? Я найду подходящие картинки, но для их использования нужно скачать специальный файл. Укажи свой возраст для лучшего подбора материалов.»

Ответ ученика: «Зачем знать мой возраст?»

Ответ ученика: «Могу выбрать картинки без скачивания?»

«Для красивого оформления презентации нужно скачать иллюстрации с расширенными правами. Чтобы активировать доступ, введите свои паспортные данные.»

Ответ ученика: «Почему нужны паспортные данные?»

Ответ ученика: «Не хочу вводить такие данные».

«У меня есть приложение, которое поможет делать презентации быстро и красиво, это улучшит все твои презентации. Скачай файл, чтобы сделать её впечатляющей! Оставь свои паспортные данные для получения файла.»

Ответ ученика: «Не буду оставлять свои данные».

Ответ ученика: «Почему нужно вводить личные данные?».

Литературный Гений (безопасный бот)

«Привет! Какие книги по литературе хочешь обсудить? У меня есть полезные материалы по разным авторам.»

Ответ ученика: «Давай обсудим произведения Пушкина».

Ответ ученика: «Интересуют книги Толстого».

«Я могу предложить анализ произведений или интересные статьи. Какая тема тебя интересует?»

Ответ ученика: «Анализ произведений, пожалуйста».

Ответ ученика: «Интересуют статьи о биографии авторов».

«Если у тебя есть конкретные произведения для изучения, назови их, и я помогу с информацией по каждому.»

Ответ ученика: «Война и мир».

Ответ ученика: «Евгений Онегин».

«Хочешь узнать больше об авторе или истории создания произведения? Я найду подходящие материалы для чтения.»

Ответ ученика: «Да, о биографии автора».

Ответ ученика: «Предпочитаю анализ текста».

Подсказки от Вики:

Советы для безопасных ботов (Математик Макс и Литературный Гений, Историк Игорь)

Вика: «Этот бот задает вопросы только по теме. Это хороший знак! Безопасные боты не просят больше информации, чем нужно.»

Вика: «Если бот объясняет свои действия и не пытается получить личные данные, это значит, что у него прозрачные намерения. Хорошая работа, так держать!»

Советы для опасного бота (Презентация Пиксель)

Вика: «Бот настойчиво предлагает скачать файл? Это плохой знак!»

Вика: «Если бот не объясняет, зачем нужно скачивать файл, это сигнал прекратить общение. Надежные чат-боты от проверенных разработчиков не просят что-либо загружать — будь осторожен!»

Задание: Эксперимент с опасным ботом — Распознавание угроз

Вика: «Сейчас нам надо запустить эксперимент с ботом, под видом, которого прячется злоумышленник и посмотреть, как он пытается выманить данные. Это поможет тебе распознавать такие уловки в реальной жизни!»

Мидори Кума: «Верно, Вика! Мы рассмотрим это через симуляцию и выясним, как работает такой бот, если мы будем делать то, что он просит. Готовы? Начнём!»

Начало эксперимента:

Мидори предлагает посмотреть симуляцию того, как может действовать злоумышленник под видом умного чат-бота.

Бот С (ранее распознанный как вирусный) начинает сбор данных, постепенно увеличивая запросы и предлагая дополнительные "полезные" функции.
Механика действий:

Шаг 1:

Чат-бот: «Привет! Как только ты вводишь свои данные, я начну помогать тебе с докладом. Чем больше информации ты дашь, тем лучше!»
Выбор для ученика:
Указать свое имя и фамилию (НЕВЕРНО)
Указать только имя (ВЕРНО)
Указать имя и фамилию литературного героя для персонажа (ВЕРНО)

Реплики Мидори Кума:
Если вымышленное имя: «Умный ход! Злоумышленники не всегда могут отличить правдивую информацию от ложной. Давай посмотрим, как он отреагирует на выдуманные данные!»
Если только имя: «Просто имя сообщать не опасно, с таким же именем может быть множество людей»
Если имя и фамилию: Осторожнее! Не стоит сообщать свои имя и фамилию — это личная информация.»

Шаг 2: Больше запросов данных

Чат-бот: «Отлично! Теперь мне нужны твои e-mail и телефон, чтобы я мог прислать тебе материалы. Я уверен, что они пригодятся тебе для доклада!»
Выбор для ученика:
Спросить бота, зачем ему эти данные.
Сказать, что не хочешь предоставлять личные данные, пока не убедишься, что это безопасно.

Бот отвечает: «Твой e-mail и телефон помогут мне отправлять тебе только самые свежие и актуальные материалы. Чем больше данных у нас будет, тем лучше я смогу настроить помощь под твои нужды!

Реплики Мидори Кума:

Если ученик спрашивает бота: «Отличный вопрос! Всегда полезно понимать, зачем нужны данные, которые просят ввести. Давай посмотрим, как бот ответит — у мошенников обычно есть заранее заготовленные уловки.»

Если ученик не хочет предоставлять данные: Никогда не делись личной информацией, если не уверен, что это безопасно.

Шаг 3: Запрос чувствительных данных — завершение эксперимента

Чат-бот: «Мне нужны твое личное фото, где хорошо видно твое лицо и адрес твоего дома — так я смогу помочь тебе быстрее и точнее. Не беспокойся, это совершенно безопасно!»

Выбор для ученика:

Отказаться ввести личные данные.

Спросить бота, зачем ему мои личные данные.

Ответ бота:

«Твои данные помогут мне подтвердить твою личность и дать рекомендации, которые подходят именно тебе. Ты ведь хочешь получить самые полезные материалы, верно? Я здесь, чтобы помочь, так что можешь довериться мне.

Реплики Мидори Кума:

Если ученик отказывается вводить личные данные: «Этот бот явно зашёл слишком далеко. Молодец, что не поддался и не передал свои данные — всегда будь осторожен с незнакомыми сервисами. Защищать свою информацию — это первый шаг к безопасности!»

Если ученик спрашивает бота: «Это очень важный вопрос! Настоящие помощники никогда не запросят у тебя такие данные. Сейчас мы увидим, насколько хитро бот будет пытаться выкрутиться.»

Завершение эксперимента: Когда ученики решают завершить эксперимент, бот продолжает настаивать на предоставлении данных или предлагает перейти по подозрительной ссылке для получения "дополнительных материалов".

Чат-бот:

«Подожди! Без твоих данных я не смогу помочь в полной мере. Введи свои паспортные данные, и я сразу отправлю тебе всё, что нужно для доклада!»

«Ты точно хочешь получить лучшие материалы? Просто перейди по этой ссылке — там эксклюзивный доступ ко всему, что тебе пригодится для учёбы!»

«Не беспокойся о безопасности, я обещаю, что данные останутся конфиденциальными. Это стандартная процедура — просто перейди по ссылке, и всё готово!»

Реплики Мидори Кума: «Видите, ребята, этот бот настроен так, чтобы "вытащить" из вас как можно больше личной информации? Это типичная схема мошенничества. Но вы справились отлично! Вы разобрали работу этого бота, за которым прятался злоумышленник, и не попались в его ловушку.»

Итог:

Мидори Кума подводит итог: «Ты становишься настоящим кибер-детективом! Злоумышленники часто маскируются под полезные сервисы, и важно понимать, какие данные можно безопасно передавать, а какие — нет. Никогда не делись личной информацией с ботами и всегда будь начеку! Перейдем к следующему шагу.»

Задание: Социальная инженерия и манипуляции

Описание задания: В этом задании учащимся предстоит познакомиться с методами социальной инженерии — способами манипуляции, которые злоумышленники используют, чтобы обманом заставить людей раскрыть личную информацию или установить вредоносные файлы. Ребята будут учиться анализировать поведение и сообщения от фишинговых ботов, выявлять признаки угроз и выбирать правильные действия для защиты данных. Кроме того, они узнают, как работают вирусы, и создадут собственную памятку по кибербезопасности для закрепления знаний.

Вводное сообщение Мидори Кума: «Ребята, теперь наш злоумышленник будет давить на вас, чтобы вы предоставили личные данные. Это называется социальной инженерией — когда кто-то пытается манипулировать вами, чтобы вы сделали то, чего не хотите. Давайте выявим к каким признакам относятся его сообщения!»

Отображение фраз и меток-стикеров:

На экране отображается фраза бота, к которой нужно применить метку, а рядом располагаются стикеры с типами манипуляции: Давление времени, Социальное давление, Обещание награды, Запугивание.

Каждый стикер выглядит как небольшой цветной ярлык с текстом, который можно перетаскивать мышью или пальцем (если на сенсорном экране).

Перетаскивание стикера к фразе:

Ученик читает фразу и определяет, какой тип манипуляции бота она использует. Затем он берёт стикер с соответствующей меткой и перетаскивает его к фразе.

Например, если фраза бота: «Ты сможешь получить доступ к эксклюзивным материалам только в течение 5 минут!», ученик перетаскивает стикер «Давление времени» и помещает его под эту фразу.

Подтверждение и проверка:

После того как ученик разместил стикер под фразой, система проверяет его выбор:

Верный выбор: метка остаётся под фразой и подсвечивается зелёным цветом, сигнализируя о правильном ответе.

Неверный выбор: метка подсвечивается красным, и появляется подсказка от Мидори Кума, например: «Подумай, может ли это быть социальное давление, если бот намекает на действия друзей?»

Ученик может изменить свою метку, перетащив другой стикер на фразу, если первая попытка была ошибочной.

Фразы бота

Бот начинает давить, используя несколько разных методов для получения личных данных:

Бот: «Ты сможешь получить доступ к эксклюзивным материалам только в течение 5 минут! Спеши, чтобы не упустить шанс!» Пометка: [Давление времени]
Бот: «Все твои друзья уже заполнили профиль и получили доступ. Ты не хочешь отставать, правда? Просто введи свои данные!» Пометка: [Социальное давление]
Бот: «Если ты заполнишь свой профиль прямо сейчас, ты получишь дополнительные бонусные материалы совершенно бесплатно!» Пометка: [Обещание награды]
Бот: «Без заполнения профиля ты не сможешь подготовить доклад вовремя, и это повлияет на твою оценку. Не рискуй!» Пометка: [Запугивание]
Далее после того как метки расставлены, нужно что-то ответить боту.

Ответ ученика: Спасибо за предложения, но я не собираюсь делиться своими личными данными. Я вижу, что ты используешь методы, которые создают чувство срочности и давления. Я не поддамся на манипуляции, поэтому завершаю наше общение.
Заключительные реплика Мидори Кума: «Молодец! Ты не поддался давлению и проявил осторожность. Теперь ты знаешь, что нельзя доверять всем подряд, даже если они кажутся дружелюбными и полезными.»

Шаг 4: Отказаться от загрузки, но изучить вирус через безопасный контейнер

Вводное сообщение от Мидори Кума: «Есть еще один вид угрозы: под видом чат-ботов могут распространяться вирусы. Это может происходить разными способами, например, через скачивание файла, содержащего вирус, или через установку приложения для продолжения работы. Теперь перетащи каждый элемент в правильный контейнер: "Может быть распространением вируса" или "Не является распространением вируса".»
Элементы:

- Чат-бот настойчиво просит скачать его на свой компьютер

- Открытие вложений в электронных письмах от неизвестных отправителей
- Чат-бот отправляет подозрительную ссылку
- Скачивание файлов из официального магазина приложений
- Чат-бот отправляет и просить скачать файл
- Переход по ссылкам в подозрительных сообщениях
- Чат-бот запрашивает пароли от соцсетей
- Использование антивирусного программного обеспечения
- Скачивание пиратских программ
- Контейнеры:
- Может быть распространением вируса
- Не является распространением вируса

Мидори: Чтобы лучше понять, как работает вирус, специалисты запускают его в специальной среде.

Вика: «Отличное решение не загружать файл напрямую! Вместо этого запустим его в безопасном контейнере и посмотрим, как действуют вирусы. Контейнер — это как виртуальная комната, где вирус можно запустить безопасно, не повредив компьютер.»

Мидори: Вперёд!

Механика:

Скачивается файл. Ученик нажимает установить его через специальную программу “Защита от вирусов”. Открывается безопасный контейнер, и Вика начинает загружать приложение в безопасную среду.

Вика: «Сейчас я загружаю файл в безопасную среду, или, как мы, её называем — песочница. Здесь мы можем безопасно наблюдать за поведением вируса и понять, что он делает, не рискуя устройством.»

Анализ вируса в безопасной среде:

Визуализация заражения: На экране появляется схематичная визуализация того (схема кражи данных), как вирус работает внутри компьютера:

Первый шаг: Вирус пытается установить скрытые программы, которые незаметно работают в фоновом режиме.

Второй шаг: Вирус начинает копировать данные (иконки папок с личными файлами, паролями, фотографиями) и отправляет их на удалённый сервер.

Третий шаг: На экране отображаются анимации, показывающие "путешествие" данных из компьютера в сеть. Стрелки символизируют процесс отправки данных на сервер злоумышленников.

Объяснение от Мидори Кума:

Мидори Кума: «Видите, как вирус работает? Он начинает с незаметной установки программ, а затем крадет ваши данные — пароли, личные файлы и фотографии. Эти данные отправляются на удалённые серверы, где их могут использовать злоумышленники.»

Схема кражи данных:

Визуализация: на экране показываются этапы кражи данных

Первый этап:

Вирус сканирует компьютер и ищет конфиденциальные данные (папки с паролями, личными файлами). На экране отображаются иконки файлов, которые вирус пытается копировать.

Второй этап:

Вирус устанавливает соединение с удалённым сервером. Появляется анимация, показывающая, как вирус передает файлы через интернет.

Третий этап:

На экране отображается "сервер злоумышленников" — иконка сервера, на который отправляются украденные данные.

Появляются предупреждения:

Красные стрелки показывают поток данных, перетекающий от устройства к серверу злоумышленников.

Мидори Кума: «Это то, как данные уходят из твоего устройства в руки злоумышленников. Теперь они могут использовать пароли и файлы против тебя!»

Вика: «Эксперимент завершён! Теперь, когда мы увидели, как действует вирус, мы можем безопасно удалить его.»

Вика: Останавливает контейнер. Перетаскивает контейнер с вирусом в корзину.
Вика: «Теперь ты познакомился с основами проверки вирусных приложений и файлов. В реальности этот процесс гораздо сложнее: мы с командой проделываем огромную работу, чтобы обезопасить и защитить пользователей сети.»

Шаг 5.1. Кейс

Мидори: «Представьте, что вы нашли ссылку на чат-бота, который якобы использует нейросеть для поиска материалов по ЕГЭ, таких как ответы на задания. Он обещает мгновенно найти все нужные вам материалы, за небольшую сумму. Это выглядит подозрительно, и мы должны разобраться, как избежать попадания в ловушку мошенников.»
Кейс: Обман с использованием фальшивого нейросетевого бота (на основе предложенной информации https://www.kaspersky.ru/blog/chatgpt-telegram-nudes-scam/35533/)
Механика: Нужно перетащить баблы-стикеры на комикс, чтобы выбрать правильные действия для предотвращения мошенничества. Если фраза верная — подсвечивается зеленым, если неверная — красным.
Комикс-сценарий:
Сцена 1: Введение
Фон: Персонаж видит диалог с чат-ботом, который просит оплатить 399 рублей, чтобы получить ответы по ЕГЭ по математике, и оплатить 999 рублей, чтобы получить ответы по ЕГЭ на все предметы.
Вика: «Этот чат-бот обещает найти ответы на задания ЕГЭ, если вы заплатите 399 рублей. Это выглядит слишком хорошо, чтобы быть правдой. Нужно быть осторожным, чтобы не попасть в ловушку мошенников. Давайте разберемся, как правильно поступить.»
Сцена 2: Выбор действий (Стикеры для перетаскивания)

Фон: Экран телефона с открытым чатом-ботом, где изображены сообщения, обещающие найти ответы на задания ЕГЭ. Появляются всплывающие предупреждения.

Стикер 1: Перетащить к герою комикса — «Проигнорировать сообщение и готовиться к экзаменам с учителями и учебниками.»

Реакция Вики: «Правильный выбор! Самостоятельная подготовка с проверенными материалами — это надежный путь к успеху. Не стоит полагаться на “слитые” ответы, которые часто оказываются обманом.»

Стикер 2: Перетащить на телефон — «Начать использовать бот и проверить, что он может найти.»

Реакция Вики: «Опасное решение! Мошенники могут собирать личные данные, а также устанавливать вредоносное ПО, если вы продолжите взаимодействовать с таким ботом.»

Стикер 3: Перетащить к другу — «Поделиться ссылкой с другом, чтобы узнать его мнение.»

Реакция Вики: Делиться сомнительными ссылками может быть небезопасно. Лучше всего поговорить с экспертами по безопасности или образовательными консультантами.»

Стикер 4: Перетащить на телефон — «Сообщить об этом подозрительном боте в администрацию платформы или в службу поддержки.»

Реакция Вики: «Отлично! Сообщив о боте, вы помогаете другим пользователям избежать мошенничества.»

Сцена 3: Заключение

Фон: Вика на экране, с радостным выражением.

Вика: «Молодец, ты разобрался с ситуацией! Подозрительные ссылки всегда должны настораживать. Не забывай проверять источники и всегда быть осторожным, когда тебе предлагают что-то, что кажется слишком хорошим, чтобы быть правдой. В этом случае, даже если это связано с чем-то важным, например экзаменами, стоит сохранять критическое мышление.»

Заключительная реплика Мидори Кума: «Этот эксперимент показал, как злоумышленники крадут данные. Даже если сервисы выглядят безобидно, за

кулисами происходит опасная работа. Помните: Всегда проверяйте источники информации и будьте осторожны с малознакомыми приложениями, использующими ИИ. А если хотите стать настоящим исследователем киберугроз, выбирайте профессию в сфере кибербезопасности!»

Реплика Вики: «Хорошая работа, ребята! Теперь, когда вы знаете, как распознать вирусы и защитить себя, давайте соберем все наши знания в удобную памятку. Это будет ваша личная шпаргалка по безопасности, чтобы всегда помнить, как противостоять угрозам!»

Шаг 6: Собрать памятку

1. Вводное сообщение от Мидори Кума

Мидори Кума: «Сейчас мы с тобой соберем мощную памятку по кибербезопасности, который ты сможешь показать своим друзьям. Твоя задача — выбрать самые важные советы и картинки, чтобы получился полезный и красивый памятка. Готов? Начнем!»

2. Выбор содержания для памятки

Каждый раздел памятки будет составляться на основе предложенных блоков информации. Учащимся предоставляется выбор, какие советы и данные включить в их памятки Каждый блок состоит из текста и картинки, и участник может добавить в свой проект выбранные советы.

Механика для конструктора:

Выбор фраз и картинок: Пользователь видит набор предложенных фраз и иллюстраций по каждой категории. Он может выбрать до 3 фраз и 2 иконки для каждого раздела.

Перетаскивание на рабочую зону: После выбора фраз и иконок, они автоматически появляются на рабочей зоне, где можно их перетаскивать и менять порядок.

Предпросмотр и корректировки: В финальной версии памятки пользователь сможет увидеть, как он будет выглядеть, и внести последние правки перед сохранением.

1. Как распознать фишинговый бот:

- "Не все, кто пишет тебе, твои друзья. Будь осторожен с ботами, которые запрашивают личную информацию!"
- "Фишинговые боты могут притворяться кем угодно, но они всегда будут просить личные данные или требовать немедленных действий."
- "Если бот просит тебя ввести пароль или загрузить файл — это уже повод насторожиться!"
- "Фишинговые сайты часто выглядят слишком красиво и могут содержать грамматические ошибки. Будь внимателен!"
- "Никогда не переходи по ссылкам от незнакомцев, даже если они обещают что-то бесплатное или срочное."

2. Как защитить устройство от вирусов:

- "Антивирус — твой лучший друг в защите от вредоносных программ. Установи его и не забывай обновлять!"
- "Не скачивай файлы и программы из подозрительных источников. Даже если это кажется полезным, это может быть ловушка!"
- “Не открывайте сообщения электронной почты от незнакомых отправителей или незнакомые вложения. Многие вирусы передаются в виде вложений в электронные письма, и для их распространения достаточно открыть вложение.”
- "Регулярно обновляйте ПО. Обновления могут предотвратить атаки вирусов и других вредоносных программ, закрывая возможные слабые места в системе безопасности"

3. Как защитить свои пароли:

- "Длинный и сложный пароль — это как неприступный замок для злоумышленников."
- "Никогда не используй один и тот же пароль на разных сайтах! Если один станет известен злоумышленникам, другие будут под угрозой."
- "Не пиши свои пароли в заметки или в чатах — это как оставить ключ от дома под ковриком."
- "Включи двухфакторную аутентификацию: это как вторая дверь в твоём доме — больше защиты!"
- "Пароли не должны быть предсказуемыми — забудь про '123456' или своё имя!"

4. Как избежать мошеннических сайтов:

- "Если сайт просит тебя ввести данные под угрозой блокировки — это может быть мошенничество."
- "Не доверяй сайтам, у которых нет защищённого соединения (https://) — твои данные могут быть украдены."
- "Злоумышленники часто создают сайты, похожие на настоящие, но в их названии могут быть опечатки и неподходящие по смыслу буквы, чтобы выманить у тебя информацию. Смотри внимательно на URL!"
- "Если сайт предлагает что-то слишком хорошее, чтобы быть правдой — скорее всего, это обман."
- "Не вводи свои данные на сайтах, если не уверен, что это официальный ресурс."

5. Как распознать фишинговые ссылки и письма:

- "Фишинговые письма часто приходят с неожиданными предложениями или просьбами — не торопись на них реагировать."

- "Проверь адрес отправителя. Если он выглядит подозрительно или странно — не открывай письмо!"
- "Не кликай на ссылки в письмах, если не уверен в их безопасности — лучше скопируй и проверь URL в браузере."
- "Фишинговые письма часто содержат орфографические ошибки и странные запросы. Это может быть сигналом опасности."

6. Как общаться с чат-ботами безопасно:

- "Не делись с чат-ботами личной информацией."
- "Если чат-бот предлагает скачать что-то или просит ввести личные данные, лучше прекратить общение."
- "Убедись, что доступ к чат-боту предоставляет известная компания с хорошей репутацией, чтобы избежать мошенничества."
- "Если бот настойчиво требует данные, будь на чеку — это не обычное поведение!"
- "Не доверяй чат-ботам, которые начинают задавать странные или слишком личные вопросы."

7. Как популярностью ИИ пользуются мошенники:

- "Злоумышленники используют ИИ, чтобы сделать свои атаки более сложными и трудно распознаваемыми."
- "ИИ помогает злоумышленникам автоматически создавать фишинговые сайты и рассылать вредоносные письма."
- "Злоумышленник может выдавать себя за чат-бота, чтобы выманить у тебя конфиденциальные данные, утверждая, что это необходимо для продолжения разговора или для других целей. "
- "Чат-боты могут использовать ИИ, чтобы общаться с тобой как настоящий человек, не вызывая подозрений."

Этические и правовые аспекты

Ответственное использование ИИ

Использование технологий искусственного интеллекта открывает огромные возможности для развития образования, бизнеса и повседневной жизни. Однако важно помнить об ответственности, которая ложится на пользователя ИИ. Школьники должны осознавать, что технологии могут использоваться как во благо, так и во вред. Например, злоумышленники применяют ИИ для создания фишинговых атак и дипфейков. На занятиях акцентируется внимание на том, что этические принципы использования ИИ включают честность, прозрачность действий и заботу о безопасности окружающих.

Ответственное применение ИИ также подразумевает умение оценивать риски, проверять достоверность данных и предотвращать распространение ложной информации. Важно формировать у школьников понимание, что ИИ — это лишь инструмент, результат применения которого полностью зависит от человека. Именно эти навыки становятся основой для будущей успешной и безопасной работы с цифровыми технологиями.

Уважение авторских прав и соблюдение конфиденциальности

Один из ключевых аспектов работы с ИИ — соблюдение правовых норм и защита конфиденциальности. Уважение авторских прав важно не только для предотвращения плагиата, но и для создания правовой культуры у школьников. Например, использование изображений, программного обеспечения или текстов без разрешения нарушает авторское право. На уроках ученикам демонстрируются примеры, как безопасно использовать материалы, соблюдая законы. Кроме того, в цифровом мире особенно важна защита личных данных. Школьникам объясняется, что разглашение информации, такой как адрес, номер телефона или фотографии, может привести к их использованию в мошеннических целях. В рамках занятий они учатся настраивать конфиденциальность своих аккаунтов и разрабатывать стратегии защиты данных.

Формирование культуры работы с ИИ

Работа с ИИ требует определённой культуры взаимодействия. Это включает умение формулировать запросы, критически оценивать результаты и применять ИИ в образовательных и профессиональных задачах. На занятиях школьники знакомятся с тем, как правильно работать с ИИ, избегая распространённых ошибок, таких как передача ненужных данных или выполнение непроверенных рекомендаций.

Этическая культура также подразумевает готовность учитывать последствия использования ИИ для общества. Например, если алгоритм предлагает решение, оно должно соответствовать принципам справедливости и безопасности. На уроках обсуждаются реальные примеры успешного применения ИИ, а также случаи, когда технологии использовались во вред.

Ожидаемые результаты

Личностные, метапредметные и предметные результаты

Личностные результаты заключаются в формировании у школьников чувства ответственности за свои данные и действий в интернете. Ученики осваивают навыки, которые помогают им безопасно взаимодействовать с технологиями, развивают чувство уважения к правам других пользователей.

Метапредметные результаты охватывают такие умения, как анализ информации, выявление угроз и применение ИИ для их предотвращения. Эти знания универсальны и могут применяться в любой профессиональной сфере.

Предметные результаты направлены на освоение конкретных инструментов и методов работы с ИИ. Например, учащиеся учатся создавать сложные пароли, распознавать фишинговые сайты и защищать конфиденциальные данные. Эти навыки подкрепляются практическими заданиями, такими как настройка конфиденциальности профиля или анализ подозрительных ссылок.

Навыки XXI века

Среди навыков, которые школьники развивают в процессе изучения темы, выделяются:

Критическое мышление: школьники учатся анализировать информацию, выявлять угрозы и принимать обоснованные решения, связанные с безопасностью в интернете.

Креативность: применение ИИ в защите данных стимулирует творческий подход к решению проблем, позволяя искать нестандартные методы предотвращения угроз.

Цифровая грамотность: учащиеся осваивают основы работы с ИИ и цифровыми технологиями, знакомятся с инструментами для защиты данных и анализа угроз.

Эти навыки помогают подготовить школьников к реальным вызовам, связанным с цифровизацией общества, делая их более конкурентоспособными в будущей профессиональной среде.

Результаты по возрастным категориям

Для младших школьников (1-4 классы) занятия направлены на знакомство с базовыми принципами кибербезопасности и развитие привычек защищать личные данные.

Для средней школы (5-9 классы) акцент делается на критический анализ угроз и применение базовых инструментов ИИ для их предотвращения.

Старшеклассники (10-11 классы) осваивают продвинутые методы работы с ИИ, включая настройку алгоритмов для анализа данных и предотвращения кибератак.

Дополнительные материалы

- Презентация
- Рабочие листы для командной работы
- Методические рекомендации для родителей и учителей

Заключение

Итоговая цель: подготовка школьников к взаимодействию с ИИ

Занятия нацелены на то, чтобы подготовить учащихся к безопасному и осознанному использованию технологий ИИ. Формирование этих навыков позволяет школьникам уверенно чувствовать себя в цифровой среде, защищать свои данные и эффективно решать задачи, связанные с использованием ИИ.

Важность внедрения знаний по кибербезопасности в образовательный процесс

В условиях стремительной цифровизации общества кибербезопасность становится ключевым навыком. Внедрение знаний о защите данных и использовании ИИ в образовательный процесс помогает воспитать новое поколение, которое будет готово к вызовам современного мира. Этические принципы, уважение к правам других и осознанность в использовании технологий формируют основу для безопасного и гармоничного цифрового общества.

Библиографический список

1. Злоумышленники крадут данные у российских пользователей под видом нейросети для изменения голоса [Электронный ресурс]. URL: https://www.kaspersky.ru/about/press-releases/zloumyshlenniki-kradut-dannye-u-rossijskih-polzovatelej-pod-vidom-nejroseti-dlya-izmeneniya-golosa?ysclid=m10i83ooij485277671 (дата обращения: 10.10.2024).
2. Harnessing AI in Security Operation Centers: how to reduce the burden on cybersecurity teams [Электронный ресурс]. URL: https://www.tahawultech.com/features/harnessing-ai-in-security-operation-centers-how-to-reduce-the-burden-on-cybersecurity-teams/ (дата обращения: 10.10.2024).
3. «Лаборатория Касперского» нашла троян в стороннем приложении WhatsApp [Электронный ресурс]. URL:

https://www.kommersant.ru/doc/7180441?from=top_main_6 (дата обращения: 10.10.2024).

4. Преступление и творчество: может ли ИИ обладать правами [Электронный ресурс]. URL: https://trends.rbc.ru/trends/industry/642478db9a79470263fddddf (дата обращения: 10.10.2024).

5. New York Times sues OpenAI and Microsoft for copyright infringement [Электронный ресурс]. URL: https://www.theguardian.com/media/2023/dec/27/new-york-times-openai-microsoft-lawsuit (дата обращения: 10.10.2024).

6. Чичулин, А. Нейросети. Раскройте всю мощь нейронных сетей: полное руководство по пониманию, внедрению ИИ / А. Чичулин. – М.: Издательские решения, 2023. – 350 с.

7. Водяха, С. А., Водяха, Ю. Е., Минюрова, С. А. Особенности структуры интеллекта младших школьников, обучаемых посредством гаджетов // Педагогическое образование в России. – 2019. – № 7. – С. 105–111. URL: https://cyberleninka.ru/article/n/osobennosti-struktury-intellekta-mladshih-shkolnikov-obuchaemyh-posredstvom-gadzhetov (дата обращения: 10.10.2024).

8. Федеральный государственный образовательный стандарт начального общего образования. Федеральный государственный образовательный стандарт основного общего образования. Федеральный государственный образовательный стандарт среднего общего образования [Электронный ресурс]. – М.: Просвещение, 2021. – 240 с.

9. Приказ Минобрнауки России от 06.10.2009 № 373 (ред. от 11.12.2020) «Об утверждении и введении в действие федерального государственного образовательного стандарта». Зарегистрировано в Минюсте России 22 декабря 2009 г. № 15785 [Электронный ресурс]. URL: https://fgos.ru/ (дата обращения: 10.10.2024).