

Государственное учреждение образования
«Средняя школа №3 г.Березы»

**Онлайн квиз по кибербезопасности в 7 классе
«CYBERQUEST: Битва за цифровую безопасность!»
Номинация «Разработка внеклассного мероприятия с применением
технологий ИИ в ходе его проведения»**

Цыганчук Анна Руслановна,
Учитель английского языка пер-
вой квалификационной категории
+375292271596
shpak.ania@yandex.ru

Пояснительная записка

Актуальность разработки внеклассного мероприятия основывается на том, что современные подростки проводят в цифровой среде значительную часть времени: социальные сети (TikTok, Telegram), игровые платформы (Roblox) и мессенджеры стали их привычным пространством. Однако именно в этой среде активно действуют «цифровые хищники» — мошенники, манипуляторы, распространители фишинга и вишинга. Воспитание цифровой гигиены и кибербезопасности становится не просто рекомендацией, а жизненной необходимостью. Проведение воспитательного мероприятия в виде командного квиза с онлайн применением технологий ИИ Qwen.ai позволяет в доступной для подростков форме привить необходимые знания и навыки распознавания и противодействия киберугрозам.

Новизна разработки. Главная инновация проведения внеклассного мероприятия в виде онлайн квиза — ИИ выступает не вспомогательным инструментом, а полноценным ведущим, судьей и генератором контента в реальном времени. Учитель не готовит вопросы заранее — их динамически подбирает Qwen.ai под заданный промпт, что обеспечивает уникальность каждого проведения и адаптацию под уровень аудитории. ИИ самостоятельно охватывает актуальные случаи из жизни (схемы обмана в Roblox, звонки от «сотрудников банка», взлом аккаунтов в Telegram). Использование Leonardo.ai для генерации авторских иллюстраций придает мероприятию современный визуальный стиль, повышает вовлеченность учащихся. Такой подход превращает традиционный квиз в живой интерактив с элементами ИИ-шоу, что соответствует интересам цифрового поколения.

Цель воспитательного мероприятия: формирование у учащихся 13–15 лет функциональной грамотности в сфере кибербезопасности через интерактивное командное соревнование с использованием технологий искусственного интеллекта.

Задачи: *образовательные:* познакомить с базовыми понятиями: фишинг, вишинг, кибербуллинг, социальная инженерия, приватность данных; научить распознавать типичные киберугрозы в повседневных цифровых сценариях; отработать алгоритмы безопасного поведения в сети. *Развивающие:* развивать критическое мышление и навыки принятия решений в условиях неопределенности; формировать коммуникативные компетенции через командное взаимодействие; стимулировать цифровую креативность и адаптивность. *Воспитательные:* воспитывать ответственность за личную цифровую безопасность и безопасность окружающих; формировать культуру этичного поведения в цифровой среде; поощрять взаимопомощь и наставничество в вопросах цифровой грамотности.

Описание используемых технологий ИИ. В разработке применяется чат-бот на базе языковой модели Qwen.ai со специально разработанным системным промптом, который обеспечивает: **генерацию адаптированных вопросов** по трем уровням сложности («Новичок» → «Профи» → «Гуру»), соответствующих возрастным особенностям и уровню подготовки учащихся;

динамическое ведение квиза: ИИ озвучивает вопросы, принимает ответы, начисляет баллы, комментирует результаты — что освобождает учителя для модерации и индивидуальной поддержки; **объективную оценку:** алгоритмическая фиксация ответов минимизирует субъективность, повышает доверие участников к результатам; **адаптивность сценария:** при необходимости учитель может корректировать темп или сложность через уточняющие запросы к ИИ в реальном времени.

Техническая доступность. Для реализации достаточно устройства с доступом в интернет (компьютер, проектор, планшет) и бесплатного аккаунта в сервисе *Qwen.ai*, что делает разработку применимой в условиях большинства общеобразовательных школ.

Ожидаемые результаты после проведения онлайн квиза с онлайн использованием ИИ: **предметные:** учащиеся знают и правильно используют 5 ключевых терминов кибербезопасности; умеют идентифицировать 8+ типичных киберугроз в смоделированных и реальных ситуациях; применяют базовые алгоритмы защиты: проверка источника, настройка приватности, создание надежных паролей; **метапредметные:** у учащихся развиваются навыки командной коммуникации, аргументации и быстрого принятия решений; формируется умение работать с информацией в условиях ограниченного времени; **личностные:** у учащихся повышается уровень цифровой ответственности; участники осознают себя активными субъектами цифровой безопасности, готовыми делиться знаниями со сверстниками и семьей;

Целевая аудитория методической разработки воспитательного мероприятия – классные руководители, педагоги-психологи, педагоги-социальные, воспитатели учреждений дополнительного образования и педагоги, работающие с учащимися подросткового возраста (13-15 лет). Готовая методическая разработка с открытым промптом для *Qwen.ai*, которую может провести любой классный руководитель, имеющий доступ к интернету и бесплатным ИИ-сервисам.

Условия реализации: воспитательное мероприятие рассчитано на 45 минут, может проводиться в кабинете информатики, медиацентре или обычном классе с проектором.

Обоснование выбора форм и методов работы. Командный квиз-квест соответствует возрастным особенностям: подростки мотивированы соревнованием, социальным взаимодействием и мгновенной обратной связью. **Игровой формат** снижает тревожность при обсуждении «взрослых» тем (мошенничество, травля). **Интерактив «Понятийный хаос»:** мультимодальное кодирование информации (слух + движение + визуал) повышает запоминание материала, снимает мышечное и психологическое напряжение. **Физкультминутка «Цифровой детокс»:** учитывает санитарно-гигиенические требования к организации занятий с использованием экранов. Формирует привычку заботиться о цифровом здоровье. **Рефлексия «Киберщит»:** визуализация личных инсайтов способствует интериоризации

знаний. Стикер-формат удобен для быстрой фиксации мысли и последующего анализа учителем. **ИИ Qwen.ai как ведущий:** снимает нагрузку с педагога при подготовке и проведении мероприятия; создаёт эффект «объективного арбитра»; вызывает эффект технологической новизны.

Обоснование отказа от традиционной методики проведения воспитательного мероприятия (лекционная форма): подростки 12–16 лет имеют клиповое мышление и низкую концентрацию на монологе. Игра с ИИ, жестами, аукционом и перехватом держит внимание динамично меняющимися активностями (каждые 3–5 минут смена деятельности).

Ход мероприятия

Этап	Деятельность учителя	Деятельность учащихся	Время
1.Организационно-мотивационный этап	Учитель приветствует учащихся. <i>-Всем добрый день, ребята! Сегодня у нас не обычная встреча. Мы находимся на стыке реальности и виртуального мира. Каждый день вы сидите в TikTok, играете в Roblox, переписываетесь в Telegram. Но знаете ли вы, что рядом с вами в сети могут бродить "цифровые хищники"? Как вы думаете, кто они?</i> Учитель стимулирует ответы учащихся. На доске закреплена иллюстрация Приложения 1 как визуализация понятия. <i>-Спасибо за вашу активность! Действительно, «цифровыми хищниками» могут быть мошенники, различными способами выманивающие у вас информацию, уговаривающие перейти по ссылке, звонящие вам и имитирующие голос знакомого человека. Был ли у вас опыт общения с «цифровыми хищниками»? Поделитесь с нами.</i> <i>-Сегодня мы не просто поговорим об этом. Мы проведем битву! У нас есть уникальный помощник — Искусственный Интеллект. Он будет ведущим, судьей и генератором задач. Ваша задача — доказать, что вы — элита цифровой безопасности. Добро пожаловать на CyberQuest!</i> На доске висит большая иллюстрация логотипа игры из электронного Приложения 2.	Приветствуют учителя. Предполагают, кем бывают «Цифровые хищники». Рассказывают о случаях общения с «цифровыми хищниками».	2 мин. 2 мин.
2.Ликбез. Базовые понятия цифровой и кибербезопасности.	<i>-Прежде чем вступать в битву, нужно зарядить оружие знаниями. Итак, блиц-ликбез по 5 главным терминам! Термины вы видите на доске. Давайте попробуем вместе дать определение этим понятиям. Как вы понимаете... (фишинг, вишинг, кибербуллинг, социальная инженерия, приватность данных)?</i> Учитель стимулирует ответы учащихся, дает необходимые комментарии и пояснения понятиям, используя материалы Приложения 3.	Знакомятся с основными терминами кибербезопасности и цифровой грамотности. Пытаются дать	3 мин.

Закрепление понятийного аппарата. Снятие психологического и мышечного напряжения.	Определения понятий для справки: Фишинг – попытки выманить личные данные через поддельные письма/сайты. Вишинг – голосовой фишинг (звонки от «сотрудников банка», «родственников»)). Кибербуллинг – травля в сети. Социальная инженерия – манипуляция людьми для получения доступа к информации. Приватность – настройки, которые контролируют, кто видит вашу информацию. <i>-Отлично! Теперь вы стали на шаг ближе к надежной защите своих данных и устройств. Но давайте потренируемся! Ведь враги – «цифровые хищники» - не дремлют! Проведем интерактив!</i> Проводится интерактив «Понятийный хаос». Учитель объясняет жесты для каждого понятия, которые должны показывать учащиеся: Фишинг - Руки скрестить перед собой (как «крючок»). Вишинг - Палец к уху (имитация звонка). Социальная инженерия – Покрутить головой, взявшись за нее руками (манипуляция). Кибербуллинг - Закрывать лицо ладонями. Приватность - Палец к губам «тсс». Учитель взразброс зачитывает ситуации для распознавания учащимися угроз: «Пришло письмо от „Банка“ с просьбой подтвердить пароль» (фишинг). «Звонит „сотрудник сотовой“ и просит назвать код из СМС» (вишинг). «В Roblox незнакомец пишет: дам робуксов, если скажешь пароль» (фишинг). «СМС: „Ваш аккаунт заблокирован, перейдите по ссылке“» (фишинг). «Кто-то создал фейковый аккаунт с твоим именем и пишет гадости от твоего имени» (кибербуллинг). «Твое личное фото без разрешения разослали в общий чат и добавили обидную подпись» (кибербуллинг). «В Telegram пишет „подруга“ (аккаунт взломан): пришли мне код, который пришёл	определения понятиям. Стоя отвечают жестами на ситуации, которые зачитывает учитель.	3 мин.
---	--	--	---------------

	тебе в СМС, я случайно указала твой номер» (социальная инженерия – манипуляция). «На сайте предлагают пройти опрос и получить скидку, но сначала заполнить анкету с паролем от почты» (социальная инженерия – манипуляция). «Ты опубликовал в открытом аккаунте фото своего пропуска в школу» (угроза приватности). «Ты используешь одинаковый пароль для всех сайтов» (угроза приватности). <i>-Отлично! Мы заложили супер базу наших кибер знаний. Самое время пройти состязание квеста!</i>		
3. Основной этап. Проведение командного квеста с использованием ИИ. Проводится Раунд 1 «Новичок»: 5 вопросов, базовая безопасность. Раунд 2 «Профи»: 5 вопросов, механика «Аукцион».	<i>-Для прохождения квеста вам нужно разделиться на команды по 4-5 человек и выбрать капитана, который будет поднимать табличку с вариантом ответа. Придумайте крутое название для вашей команды!</i> <i>-Правила просты. Я запускаю ИИ чат Qwen.ai и ввожу в него специально разработанный промпт. Сам ИИ чат будет и генератором вопросов, и ведущим нашего квеста, и судьей.</i> <i>-И помните. В этом квесте нет выигравших и проигравших, ведь самое главное – это умение выстроить вашу «киберкрепость», чтобы противостоять всем угрозам!</i> <i>-Итак, команды готовы? Я запускаю квест!</i> Учитель вводит в заранее подготовленный сервис ИИ Qwen.ai промпт, который запускает квест из электронного Приложения 7. Роль учителя при его проведении – контролирующая и консультирующая. Учитель озвучивает раунды, вопросы, варианты ответов, полученные командами баллы и т.д. Иллюстрации раундов из электронного Приложения 5 находятся на доске.	Делятся на команды, выбирают капитанов, придумывают названия командам. Обучающиеся проходят раунды квеста в командах.	2 мин. 10 мин.
4. Физкультминутка	После Раунда 2 «Профи» учитель делает паузу в игре и предлагает учащимся выполнить расслабляющую гимнастику для глаз.	Выполняют гимнастику для глаз.	3 мин.

	<i>-В любом деле важна «свежая голова» и «четкий взгляд». Давайте сделаем паузу, расслабимся и «перезапустим» наш мозг.</i> Проводится физкультминутка «Цифровой детокс». Под спокойную расслабляющую музыку учитель дает инструкции учащимся: «Выключение экрана»: Крепко зажмурить глаза на 5 секунд, широко открыть. (Повторить 3 раза). «Скроллинг вверх»: Плавно поднять глаза вверх, затем вниз. (Повторить 3 раза). «Удаление вируса»: Активные встряхивания кистями рук, как будто стряхиваете воду. «Перезагрузка тела»: Потянуться вверх всем телом, вдох, на выдохе расслабленно опустить руки. «Режим полета»: Сделать глубокий вдох, задержать дыхание, медленно выдохнуть. <i>-Отлично! Все системы и режимы «перезапущены». Пора продолжить наши состязания.</i>		
5. Продолжение Основного этапа. Проводится Раунд 3 «Гуру»: 5 вопросов, механика «Перехват» (кто быстрее). Финальный блиц: 3 вопроса на скорость.	Проводятся оставшиеся раунды. Подводятся итоги, определяется победитель квиза. Учителю важно подчеркнуть посыл о том, что квиз носит развлекательный характер и его главная цель для учащихся – это приобретение знаний и навыков о киберугрозах и методах противостояния им.	Отвечают на вопросы оставшихся раундов.	6 мин.
6. Подведение итогов квиза.	<i>-Итак, наш квиз окончен! Я благодарю все команды за участие! Вы сражались со всеми киберугрозами как настоящие защитники информационного пространства! Я желаю вам никогда не сталкиваться с ними, но всегда</i>	Подводят итоги квиза. Получат памятки по	3 мин.

Рефлексия	<i>быть на страже и учить кибербезопасности своих знакомых и близких.</i> <i>-А победителем нашего квиза является команда ! Вы получаете медали киберзащитников! Так держать!</i> Учитель награждает победителей квиза, вешает им «Медали». Всем участникам квиза раздаются памятки по кибербезопасности из электронного Приложения 6.	кибербезопасности.	
	<i>-Я очень надеюсь, что кибер квиз увлек вас и вы приобрели много знаний и умений. Давайте подытожим все наши навыки. Я хотела бы услышать от вас обратную связь. Что бы вы положили в свой «Киберщит»? Напишите, пожалуйста, ответы на стикерах и приклейте их к «Киберщиту».</i> Иллюстрация «Киберщита» из электронного Приложения 4. <i>-Спасибо вам за участие и активность! До новых встреч!</i>	Осуществляют рефлексию своей деятельности. Приклеивают стикеры к «Киберщиту»	2 мин.

Список используемой литературы

1. Хабибуллин И. Р., Азовцева О. В., Гареев А. Д. Актуальность использования нейросетей в образовательных целях // Молодой ученый. 2023. № 13 (460). С. 176-178.
2. Шамсутдинова Т. М. Проблемы и перспективы применения нейронных сетей в сфере образования // Открытое образование. 2022. Т. 26. № 6. С. 4-10.
3. Шобонов Н.А., Булаева М.Н., Зиновьева С.А. Искусственный интеллект в образовании. Проблемы современного педагогического образования. 2023; № 79-4: 288–290.

Приложение
Ссылка и QR код к электронным приложениям воспитательного мероприятия

https://drive.google.com/drive/folders/10N9ANUkPvTWyKHX_xxJ21ljtl-vlMDIU?usp=sharing

