

Государственное учреждение образования
«Давыдовская средняя школа»

Конспект занятия по информатике
«Нейросети и информационная безопасность»
в 11 классе

Номинация: разработка урока с применением технологий ИИ
в ходе проведения учебного занятия

Автор:
Маркевич Светлана Сергеевна, учитель
информатики высшей
квалификационной категории

e-mail svetl@schooldavydovka.by

Пояснительная записка

Актуальность. Современные цифровые инструменты с использованием искусственного интеллекта становятся неотъемлемой частью различных сфер жизни от образования и науки до развлечений, бизнеса и искусства. Они предоставляют уникальные возможности для решения исследовательских, научных и творческих задач, что делает их полезными помощниками в учебе и будущей профессии. Умение использовать такие технологии становится важным навыком, который поможет будущим специалистам быть конкурентоспособными на рынке труда. Однако вместе с этим растет и необходимость осознания того, что нейросети – это мощный инструмент, который требует ответственного подхода. Искусственный интеллект – сложная технология, которая может использоваться как во благо, так и во вред. Например, ИИ уже применяется для создания фейковых новостей, фишинговых атак и автоматизированного взлома систем.

Изучение этих аспектов в школе позволяет сформировать у учащихся осознанный подход к использованию технологий искусственного интеллекта. Школьники должны не только уметь применять нейросети для учебы и проектов, но и понимать, какие риски они несут, должны научиться распознавать потенциальные угрозы. Знание основ информационной безопасности поможет им защитить себя в цифровом мире и использовать ИИ ответственно. Таким образом, формирование представлений о возможностях и рисках использования ИИ является актуальной задачей.

Целевая аудитория: 11 класс

Цель урока: Обобщить и систематизировать знания учащихся о цифровой и кибербезопасности, закрепить представления о возможностях и рисках использования нейросетей в контексте информационной безопасности, а также способах защиты от потенциальных угроз.

Задачи урока:

<i>Образовательные</i>	Рассмотреть понятия «нейросеть», «информационная безопасность», «кибербезопасность». Изучить возможности и риски использования нейросетей. Научить применять нейросети для решения практических задач. Проанализировать потенциальные угрозы информационной безопасности, связанные с использованием нейросетей.
<i>Развивающие</i>	Развивать навыки работы с современными технологиями, включая использование нейросетей. Совершенствовать умение анализировать, сравнивать и систематизировать информацию. Развивать умение выполнять групповые проекты.
<i>Воспитательные</i>	Воспитывать ответственное отношение к использованию цифровых технологий. Формировать осознание важности информационной безопасности в современном мире. Прививать навыки этичного и безопасного использования ИИ-технологий. Стимулировать интерес к изучению современных технологий.

Описание используемых технологий ИИ:

Технология	Инструментарий
Генерация текста	DeepSeek, Qwen2.5-Max, GPT-4.1 mini
Интерпретация понятий, разъяснение их сути	
Анализ текста, генерация текста с заданными параметрами (вопросы теста)	
Генерация майнд-карт (интеллект-карт)	Mapify
Генерация программного кода в заданной среде программирования	BLACKBOXAI

Ожидаемые результаты урока:

Предметные	Могут объяснить основные понятия Имеют представление о возможностях и потенциальных угрозах использования нейросетей и путях их минимизации
Метапредметные	Владеют навыками анализа и сопоставления информации Используют нейросети для решения практических учебных задач Совершенствуют умение презентовать результаты своей учебной работы
Личностные	Ответственно относятся к использованию цифровых средств и инструментов Осознают важность защиты персональных данных в цифровом мире. Осознают значение безопасного и ответственного поведения при использовании цифровых ресурсов и инструментов

Обоснование выбора форм и методов работы:

Практико-ориентированный подход позволяет учащимся не пассивно воспринимать информацию, а самостоятельно анализировать информацию, что повышает вовлеченность в учебный процесс и глубину усвоения материала.

Работа в подгруппах обеспечивает охват широкого спектра подтем, развивает навыки сотрудничества и коллективного решения задач.

Работа с ИИ-инструментами готовит учащихся к реалиям современного мира, где такие технологии активно используются в науке, бизнесе и повседневной жизни, обеспечивая формирование цифровых компетенций.

Структурирование информации с помощью кругов Эйлера, схем, интеллект-карт, таблиц и тестовых заданий помогает систематизировать знания, выделить ключевые идеи и установить причинно-следственные связи.

Таким образом, выбранные формы и методы работы обеспечивают:

- формирование у учащихся умение работать с учебной информацией, анализировать и структурировать получаемые знания, включая их в систему сформированных знаний, представлений и умений;
- обеспечивают интенсификацию обучения за счет охвата разных подтем и использования инструментов искусственного интеллекта;
- способствуют формированию цифровой компетенции и основ безопасного поведения в цифровой среде.

Конспект урока

Класс: 11

Тема урока: Нейросети и информационная безопасность

Тип урока: комбинированный

Формы организации деятельности учащихся: фронтальная, групповая, индивидуальная

Цель урока: Обобщить и систематизировать знания учащихся о цифровой и кибербезопасности, закрепить представления о возможностях и рисках использования нейросетей в контексте информационной безопасности, а также способах защиты от потенциальных угроз.

Задачи урока:

Образовательные:

- Рассмотреть понятия «нейросеть», «информационная безопасность», «кибербезопасность».
- Изучить возможности и риски использования нейросетей.
- Научить применять нейросети для решения практических задач.
- Проанализировать потенциальные угрозы информационной безопасности, связанные с использованием нейросетей.

Развивающие:

- Развивать навыки работы с современными технологиями, включая использование нейросетей.
- Совершенствовать умение анализировать, сравнивать и систематизировать информацию.
- Развивать умение выполнять групповые проекты.

Воспитательные:

- Воспитывать ответственное отношение к использованию цифровых технологий.
- Формировать осознание важности информационной безопасности в современном мире.
- Прививать навыки этичного и безопасного использования ИИ-технологий.
- Стимулировать интерес к изучению современных технологий.

Оборудование:

- компьютеры;
- доступ в сеть Интернет;
- программное обеспечение: браузер, MSWord; PascalABC;
- учебник «Информатика. 11 класс»;
- карточки с тестом (Приложение 1), рабочие листы (Приложение 3).

Критерии оценки:

- Активность в обсуждении.
- Качество выполнения группового задания.
- Логичность и глубина выводов.

Ход урока

1. Организационный момент (2 мин)

Приветствие, проверка присутствующих.

Учитель: Добрый день, граждане XXI века! Как вы считаете, цифровая эпоха уже наступила?

Мы живем в уникальное время, когда технологии меняют общество кардинальным образом. Мы уже наблюдаем масштабные изменения: автоматизация процессов, искусственный интеллект, большие данные, интернет вещей – все это уже стало частью нашей повседневной жизни. Новые технологии приносят с собой и новые угрозы, поэтому так важен вопрос цифровой и кибербезопасности.

2. Проверка домашнего задания. Актуализация знаний (3 мин)

Учитель: Сегодня я предлагаю вам необычную форму проверки домашнего задания. Возьмите рабочие листы. Вы видите список вопросов, на которые надо ответить «ВЕРНО» или «ЛОЖЬ» в таблице рядом с вопросами. Если утверждение верно, оставьте ячейку таблицы пустой. Если ложно – закрасьте ее. Так каждый из вас получит свой уникальный «QR-код» проверки домашнего задания. На выполнение – 5 минут. Приступаем!

(Варианты вопросов и ответы к ним приведены в Приложении 1).

Учитель: Сейчас каждый из вас получит «контрольный QR-код». Сверьте его со своим и оцените правильность выполнения теста.

(Раздает карточки с ответами. Учащиеся выполняют самооценку).

3. Объявление темы урока и формулировка целей (2 мин)

Учитель: Сегодня у нас не просто урок, а настоящая операция в киберпространстве. Вы становитесь агентами цифровой безопасности – теми, кто защищает данные, распознает угрозы и использует передовые технологии. А также обучает население способам избежать угроз информационной безопасности.

Тема сегодняшнего занятия: «Нейросети и информационная безопасность». Как вы думаете, какие знания нам предстоит добыть, каких целей достичь в ходе урока?

(В обсуждении с учащимися формулируются учебные цели)

- Узнать возможности нейросетей.
- Проанализировать их уязвимости и риски.
- С помощью нейросетей создать инструментарий для повышения цифровой грамотности населения (собственно, учащихся).

4. Теоретическая часть (5 мин)

Учитель: Нейросети – одна из самых интересных и перспективных технологий нашего времени. Это искусственная система, которая имитирует работу человеческого мозга. Она состоит из «нейронов» (математических блоков) и «связей» между ними. Ее главная задача – находить закономерности в данных и на их основе принимать решения.

Например, нейросеть в TikTok анализирует, какие видео вам нравятся, и предлагает похожие, в беспилотных автомобилях она распознаёт пешеходов и дорожные знаки, нейросети могут создавать музыку, писать истории или даже играть в шахматы лучше человека. В середине прошлого века считалось, что признаком разумности компьютера станет умение вести с ним беседу, неотличимую от беседы с человеком. Как вы думаете, почему сегодня этот критерий безнадежно устарел? *(Обсуждение с классом, вывод: современные чат-боты иногда проходят тест Тьюринга, но это не означает наличия сознания или разума).*

Одна из самых удивительных особенностей нейросетей заключается в том, что они могут учиться. Это похоже на то, как вы учитесь в школе: чтобы понять тему, нужно решить много задач. Как и вы, нейросеть может ошибаться, но после каждой ошибки она корректирует свои «веса». Чем больше данных она обрабатывает, тем точнее становится (тренировка на миллионах примеров!).

Нейросети – это мощный инструмент, который меняет нашу жизнь. Но вместе с этим они приносят и новые вызовы. Не только добропорядочные граждане используют нейросети. Их возможности могут применить и во вред. Сегодня мы разберемся в этой проблеме на практике. Каждая группа получит свое задание. Готовы к миссии? У вас будет 20 минут на выполнение задания и подготовку выступления по его итогам.

Сейчас вы разделитесь на группы – отделы кибербезопасности. Каждый отдел получил досье с заданием (это ваши рабочие листы). Внимательно прочитайте задание и приступайте к выполнению, следуя инструкции. При работе с нейросетями учитывайте их особенности *(Приложение 2 – Советы по работе с нейросетями).*

5. Практическая работа (20 мин)

Учитель: Вы можете выбрать группу в соответствии со своими интересами, но я рассчитываю, что у нас получится не менее 5 групп.

- Аналитикам предстоит проанализировать понятия цифровой, информационной и кибербезопасности. Эта задача потребует логики.

- Дознаватели – ваша задача выяснить у нейросетей, что они умеют делать.

- Разведчики выяснят, чем опасны нейросети, как их могут использовать злоумышленники.

- Группа пропагандистов подготовит советы простым гражданам, не владеющим секретами безопасной работы в сети Интернет по безопасному использованию нейросетей.

- Группа диагностов с помощью нейросетей создаст текстовый тест по пройденным трем параграфам.

И особое задание для наших продвинутых специалистов. Кто возьмется с помощью нейросети создать и протестировать программу? (Спойлер, если вы правильно составите запрос, нейросеть создаст рабочую программу, почти не требующую отладки!).

Готовы? Приступаем! Ознакомьтесь с инструкцией в рабочих листах (*Приложение 3*) и не стесняйтесь обращаться за помощью к нейросетям и к учителю!

(*Варианты ответов нейросетей на запросы разных групп приведены в Приложении 4*).

6. Обсуждение и подведение итогов (8 мин)

Каждая группа кратко представляет результаты своей работы и делает выводы.

Учитель организует краткое обсуждение.

Совместно заполняется таблица в конспектах:

Опасности нейросетей	Пути предотвращения угроз

(*Примерный образец приведен в Приложении 5*)

7. Рефлексия. Итоги. Домашнее задание (3 мин)

Учитель: У нас был нестандартный урок, предлагаю завершить его нестандартной рефлексией. На доске вы видите «Шкалу ИИ-рисков». Как вы думаете, насколько опасны нейросети?

(На доске – шкала от 0 – «Это ерунда!» до 10 – «Это апокалипсис!»).

Ученики ставят мелом метки на шкалу, отвечая на вопрос: «Насколько опасны нейросети в руках злоумышленников?».

Обсуждение крайних оценок: «Почему ты поставил 2? А почему 9?».

Какие задания вызвали затруднения?

Где могут пригодиться полученные сегодня знания?

Учитель: На дом даю вам задание на выбор. Вы можете порассуждать (устно, письменно, в виде схемы или таблицы), как нейросети могут помочь вам лично в вашей учебе. Или, наоборот, вы можете порассуждать, как учитель догадается, что сочинение вместо вас написала нейросеть или задачу решила вместо вас. Спойлер – учитель догадается! Но как?

Благодарю вас за продуктивную и качественную работу на уроке. Хорошего вам всем настроения!

Список используемой литературы

1. Информатика : учебное пособие для 11 класса / В. М. Котов, А. И. Лапо, Ю. А. Быкадоров, Е. Н. Войтехович. – Минск, Народная асвета, 2021. – 112 с.
2. Мартынов, Д. В. Защита личной информации в чатах с нейронными сетями: анализ проблем и методов защиты при хранении информации пользователей / Д. В. Мартынов, В. С. Черников // Теория и практика современной науки. – 2024. – № 2 (104). – С. 111-116.
3. Носова, Л. С. Искусственный интеллект и нейросети в образовании : учебно-методическое пособие / Л. С. Носова. – Челябинск : Изд-во Библиотека А. Миллера, 2024. – 118 с.
4. Ортина, Н. А. Обучение школьников работе с содержательным наполнением электронных изданий: возможности и преимущества использования нейронных сетей / Н. А. Ортина // Вестник Московского городского педагогического университета. – 2024. – Серия: Информатика и информатизация образования. – № 4 (70). – С. 37-47.

Приложение 1

Проверка домашнего задания. Ответьте на вопросы «ВЕРНО» или «ЛОЖЬ» и заполните таблицу.
В случае ответа «ВЕРНО» оставьте ячейку таблицы пустой, в случае ответа «ЛОЖЬ» закрасьте ее.

1	2	3
4	5	6
7	8	9
В.1 Самооценка ____		

- 1 Основа информационного общества – использование информационных технологий во всех сферах деятельности.
- 2 Информационная культура не связана с общечеловеческой культурой.
- 3 Переход от индустриального общества к информационному сопровождается процессом информатизации.
- 4 Кибербезопасность - это состояние защищенности информационной инфраструктуры от угроз.
- 5 Эксплойт — это полезное обновление для программ.
- 6 Антивирусные программы полностью исключают риск кибератак.
- 7 Обучение пользователей не влияет на кибербезопасность.
- 8 Безопасность - это состояние защищенности только интересов личности.
- 9 Объем хранимой во всем мире информации вырос в 50 раз с 2010 по 2020 год.

Проверка домашнего задания. Ответьте на вопросы «ВЕРНО» или «ЛОЖЬ» и заполните таблицу.
В случае ответа «ВЕРНО» оставьте ячейку таблицы пустой, в случае ответа «ЛОЖЬ» закрасьте ее.

1	2	3
4	5	6
7	8	9
В.2 Самооценка ____		

- 1 Информатизация — это процесс создания условий для удовлетворения информационных потребностей общества.
- 2 Информационная цивилизация – прямая «наследница» аграрной цивилизации.
- 3 Информатизация создаёт новые рабочие места, которые доминируют в экономическом развитии.
- 4 Угроза безопасности — это произошедшее воздействие, которое всегда нарушает безопасность.
- 5 Информационная культура не связана с общечеловеческой культурой.
- 6 Обучение пользователей не влияет на кибербезопасность.
- 7 Защита информации должна обеспечивать её доступность и конфиденциальность.
- 8 Кибератака может произойти только на компьютере, но не на смартфоне.
- 9 Информационная безопасность — это состояние защищенности интересов личности, общества и государства в информационной сфере.

Проверка домашнего задания. Ответьте на вопросы «ВЕРНО» или «ЛОЖЬ» и заполните таблицу.
В случае ответа «ВЕРНО» оставьте ячейку таблицы пустой, в случае ответа «ЛОЖЬ» закрасьте ее.

1	2	3
4	5	6
7	8	9
В.3 Самооценка ____		

- 1 Информационное общество отличается низким уровнем развития микроэлектроники.
- 2 Информационная культура включает только технологические навыки.
- 3 Информатизация – использование компьютерных устройств.
- 4 Угроза безопасности — это возможность воздействия на систему, которое может нарушить её безопасность.
- 5 Безопасность — это состояние защищенности только интересов личности.
- 6 «Кибер» означает «связанный с компьютерами и Интернетом».
- 7 Уязвимость — это свойство информационной инфраструктуры, которое позволяет угрозе осуществиться.
- 8 DDoS-атака направлена на обеспечение бесперебойной работы системы.
- 9 Обеспечение кибербезопасности — это противодействие угрозам информационной безопасности.

Проверка домашнего задания. Ответьте на вопросы «ВЕРНО» или «ЛОЖЬ» и заполните таблицу.
В случае ответа «ВЕРНО» оставьте ячейку таблицы пустой, в случае ответа «ЛОЖЬ» закрасьте ее.

1	2	3
4	5	6
7	8	9
В.4 Самооценка ____		

- 1 Основа информационного общества – использование информационных технологий во всех сферах деятельности.
- 2 Информатизация — это процесс создания условий для удовлетворения информационных потребностей общества.
- 3 Процесс информатизации создаёт новые рабочие места.
- 4 Информационная безопасность не связана с защитой интересов государства.
- 5 DDoS-атаки направлены на повышение скорости работы серверов.
- 6 Антивирусные программы полностью исключают риск кибератак.
- 7 Главное уязвимое место кибербезопасности — технические неполадки.
- 8 Основная цель кибератак — получение финансовой выгоды.
- 9 Обучение пользователей не играет важной роли в обеспечении кибербезопасности.

«Контрольные QR-коды» - ответы на тест-задания

Вариант 1			Вариант 2			Вариант 3			Вариант 4		
1	2	3	1	2	3	1	2	3	1	2	3
4	5	6	4	5	6	4	5	6	4	5	6
7	8	9	7	8	9	7	8	9	7	8	9

Приложение 2

Советы учащимся по использованию нейросетей

1. Формулируйте вопросы четко и конкретно. Нейросети лучше отвечают на ясные вопросы.
2. Если ответ вас не устраивает, попробуйте переформулировать вопрос.
3. Разбивайте сложные задачи на части. Если задание большое или сложное, разделяйте его на несколько шагов.
4. Если нейросеть дала вам сложный ответ, попробуйте переформулировать вопрос или уточнить его.
5. Попросите нейросеть привести конкретные примеры.
6. Нейросети могут давать разные ответы в зависимости от контекста. Например: Ответ как биолог или Ответ как историк. Нейросеть учитывает содержание чата в ответах, значит, для новой задачи лучше начать новый чат.
7. Нейросети — это помощники, но не абсолютный авторитет. Всегда анализируйте их ответы и думайте самостоятельно.
8. Совет на будущее: Нейросети иногда могут ошибаться. Поэтому сверяйте полученные данные с надёжными источниками (учебниками, научными статьями, официальными сайтами).

Рабочий лист

Фамилия, имя _____ Класс _____

Группа: Аналитики

Задача: Проанализировать и сопоставить определения понятий «информационной безопасности», «цифровой безопасности» и «кибербезопасности» с помощью нейросети. Визуализировать их взаимосвязь в виде кругов Эйлера.

Инструмент: DeepSeek; Qwen2.5-MAX

Инструкция:

1. Откройте две или более вкладки в браузере и войдите в учебный аккаунт на сайтах нейросетей DeepSeek и Qwen2.5-MAX.
2. Спросите у нейросетей, что означают приведенные выше понятия, попросите объяснить их на понятных примерах.
3. Попробуйте предположить, какое из понятий более обширное, а какое – более узкое.
4. Представьте соотношение данных понятий в виде кругов Эйлера.
5. Попросите нейросеть создать аналогичную схему. Сравните ее с вашей – что совпало?

6. Подготовьте краткий отчет по итогам вашего рассуждения.

Рабочий лист

Фамилия, имя _____ Класс _____

Группа: Дознаватели

Задача: Проанализировать возможности нейросетей и сферы их применения. Визуализировать результат в виде интеллект-карты.

Инструмент: DeepSeek; Mapify.

Инструкция:

1. Откройте две или более вкладки в браузере и войдите в учебный аккаунт на сайтах нейросетей DeepSeek и Mapify.
2. Попросите нейросеть описать возможности современных нейросетей. Чтобы ответ не был слишком длинным, попросите дать краткий, схематичный или ограниченный количеством вариантов ответ.
3. Обсудите ответ, выделите ключевые функции, категории.
4. Представьте возможности нейросетей в виде интеллект-карты (любого вида). В центре листа напишите: «Возможности нейросетей». Добавьте ветви для каждой категории, заполните.
5. Визуализируйте! Используйте:
 - **Разные цвета** для разных категорий.
 - **Рисунки.**
 - **Стрелки** для связей.

6. Подготовьте краткий отчет по итогам вашего рассуждения.

Рабочий лист

Фамилия, имя _____ Класс _____

Группа: Разведчики

Задача: Проанализировать риски нейросетей (как их могут использовать злоумышленники). Визуализировать результат в виде интеллект-карты.

Инструмент: DeepSeek, Mapify, Qwen2.5-MAX.

Инструкция:

1. Откройте две или более вкладки в браузере и войдите в учебный аккаунт на сайтах нейросетей DeepSeek, Qwen2.5-MAX и Mapify.
2. Попросите нейросеть описать возможность мошеннического использования современных нейросетей. Чтобы ответ не был слишком длинным, попросите дать краткий, схематичный или ограниченный количеством вариантов ответ.
3. Обсудите ответ, выделите ключевые опасности.
4. Представьте опасности нейросетей в виде интеллект-карты (любого вида). В центре листа напишите: «Опасности нейросетей». Добавьте ветви для каждой категории, заполните.
5. Визуализируйте! Используйте:
 - **Разные цвета** для разных категорий.
 - **Рисунки**.
 - **Стрелки** для связей и последствий.

6. Подготовьте краткий отчет по итогам вашего рассуждения.

Рабочий лист

Фамилия, имя _____ Класс _____

Группа: Пропагандисты

Задача: Составить список советов для людей, которые мало знают о нейросетях, с помощью нейросети и оформить их в виде памятки.

Инструмент: DeepSeek; Qwen2.5-MAX

Инструкция:

1. Откройте две или более вкладки в браузере и войдите в учебный аккаунт на сайтах нейросетей DeepSeek и Qwen2.5-MAX.
2. Дайте нейросетям запросы: «Дай 5 простых советов, как обычному человеку избежать мошенничества с нейросетями», «Как распознать фейковое сообщение или звонок с использованием ИИ?», «Что делать, если кажется, что тебя обманывают с помощью нейросети?»
3. Выпишите самые понятные и полезные советы.
4. Упростите сложные формулировки, чтобы они были понятны даже детям или пожилым людям.

5. Подготовьте краткий отчет по итогам вашего рассуждения.

Рабочий лист

Фамилия, имя _____ Класс _____

Группа: Диагносты

Задача: Создать тест по параграфу учебника с использованием нейросетей.

Инструмент: DeepSeek; Qwen2.5-MAX

Инструкция:

1. Откройте две или более вкладки в браузере и войдите в учебный аккаунт на сайтах нейросетей DeepSeek и Qwen2.5-MAX.
2. Скопируйте текст параграфа из электронной версии учебника (Кибербезопасность).
3. Попросите нейросеть составить простой тест на основе данного текста.
4. Обсудите ответ, выберите наиболее удачные вопросы. Они не должны быть слишком простыми или слишком сложными (например, не стоит спрашивать у учащихся, в каком году количество данных в Интернете увеличилось вдвое).
5. Вставьте выбранные вопросы в документ MSWord, отформатируйте при необходимости, сохраните ваш тест в папке класса под своими фамилиями.
6. Подготовьте краткий отчет по итогам вашего рассуждения.

Рабочий лист

Фамилия, имя _____ Класс _____

Группа: Программисты

Задача: Создать программу для ввода вопросов и проведения тестирования в среде PascalABC с использованием нейросети.

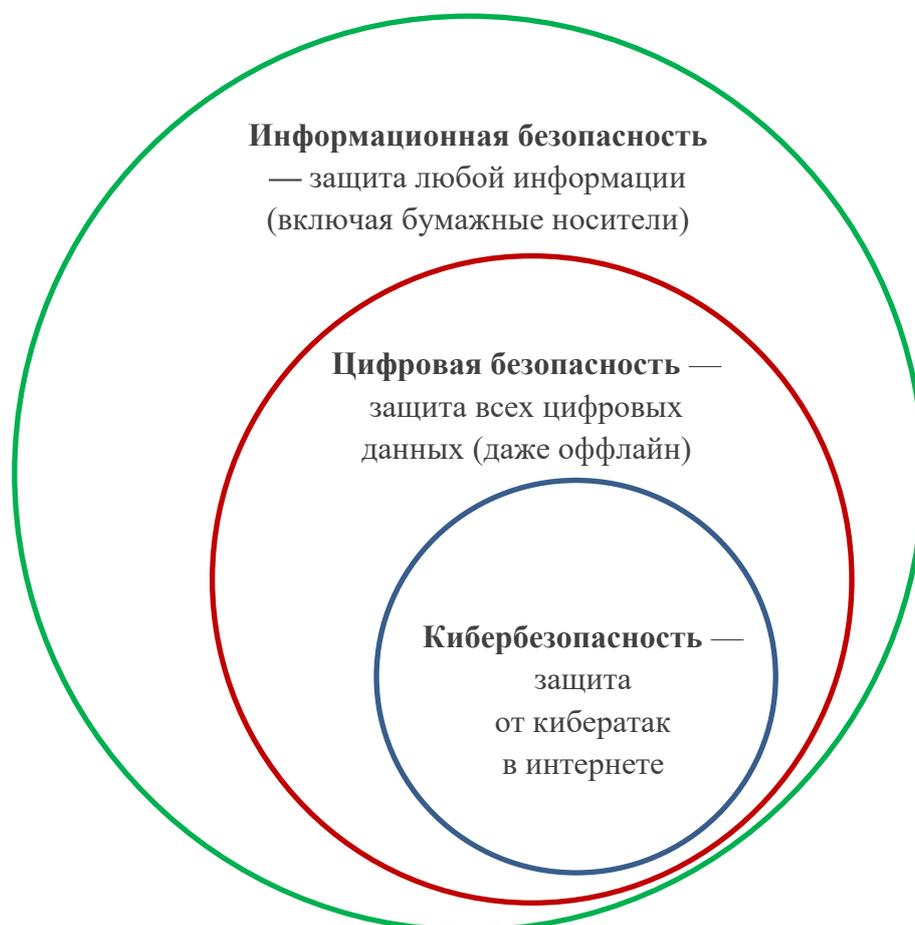
Инструмент: BLACKBOXAI

Инструкция:

1. Откройте вкладку в браузере и войдите в учебный аккаунт на сайте нейросети BLACKBOXAI. Откройте ЯндексПереводчик в отдельной вкладке.
2. Сформулируйте запрос к нейросети по составлению программы в заданной среде программирования. Продумайте, что надо указать в запросе, чтобы в программе можно было вводить вопросы и варианты ответов, выделять правильный вариант ответа, сохранять разное количество вопросов, проводить тестирование учащихся и выдавать результат тестирования.
3. Переведите запрос на английский язык и введите его в чат нейросети.
4. Скопируйте получившуюся программу и протестируйте ее в среде программирования.
5. При необходимости подкорректируйте. Сохраните программу в папке класса под вашими фамилиями.
6. Подготовьте краткий отчет по итогам вашего рассуждения.

Возможные варианты решений

Группа 1. Аналитики

**Пример ответа нейросети:**

[Информационная безопасность]

↳ включает [Цифровую безопасность]

↳ включает [Кибербезопасность]

Разница между **информационной безопасностью** и **кибербезопасностью** примерно такая же, как между защитой всех твоих секретов в жизни и защитой только цифровых данных.

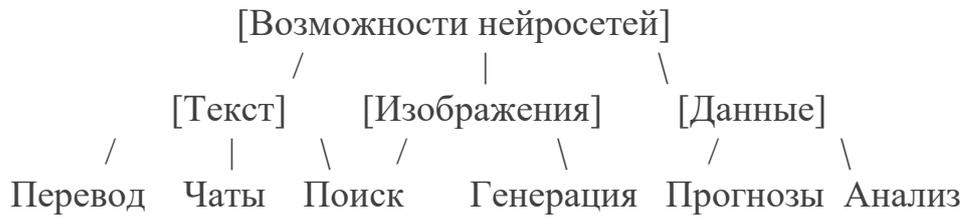
Информационная безопасность — это очень широкое понятие.

Кибербезопасность — это часть информационной безопасности, связанная только с цифровым миром.

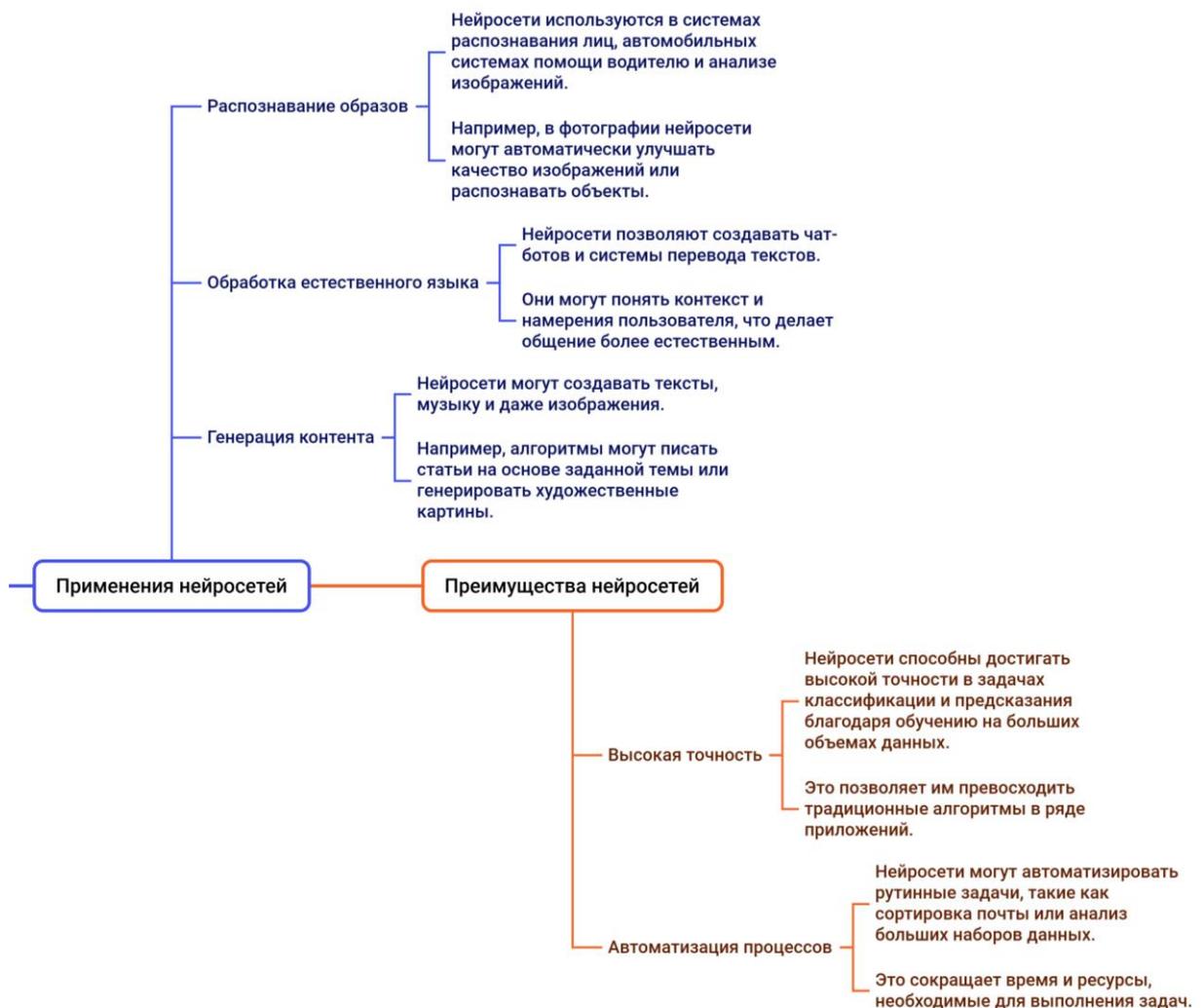
Как защита всего дома (двери, окна, сейф) vs защита только компьютера (антивирус, брандмауэр). 😊

Группа 2. Дознаватели

Ответ нейросети DeepSeek:

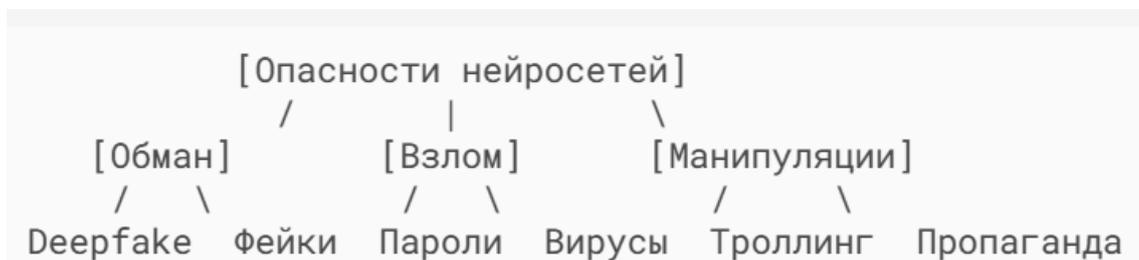


Ответ нейросети Marify



Группа 3. Разведчики

Ответ нейросети DeepSeek



Основные риски нейросетей и их использование злоумышленниками

Нейросети, несмотря на свои преимущества, могут быть опасными инструментами в руках злоумышленников. Вот ключевые риски:

1. Генерация фейкового контента (Deepfake)

- **Что делают:**
 - Создают поддельные фото, видео, аудио, имитирующие реальных людей.
- **Как используют:**
 - Распространение фейковых новостей.
 - Мошенничество (например, голосовой deepfake CEO для хищения денег).
 - Компромат и шантаж.

2. Кибератаки с помощью ИИ

- **Что делают:**
 - Нейросети автоматизируют взлом паролей, обходят капчи, находят уязвимости.
- **Как используют:**
 - Массовые DDoS-атаки.
 - Фишинг с персонализированными письмами (нейросеть анализирует жертву).
 - Вредоносные программы, адаптирующиеся под защиту.

3. Социальная инженерия 2.0

- **Что делают:**
 - Нейросети анализируют соцсети жертвы и создают убедительные сообщения.
- **Как используют:**
 - Имитация знакомых в чатах («Мама, срочно нужны деньги!»).
 - Мошенничество в службах поддержки (боты-«операторы»).

4. Манипуляция рынком и данными

- **Что делают:**
 - Генерация фальшивых отзывов, новостей для влияния на биржу.
- **Как используют:**
 - Искусственное завышение/обвал акций.
 - Фейковые рейтинги товаров.

5. Нарушение конфиденциальности

- **Что делают:**
 - Нейросети анализируют открытые данные и деанонимизируют людей.
- **Как используют:**
 - Шантаж, слежка.
 - Кража личных данных (например, для кредитов).

6. Автоматизация преступлений

- **Что делают:**
 - Боты в даркнете ищут уязвимости, продают запрещённые товары.
- **Как используют:**
 - Торговля оружием, наркотиками через ИИ-посредников.
 - Взлом систем видеонаблюдения.

7. Боты-provokatory

- **Что делают:**
 - Нейросети массово генерируют пропаганду, троллинг.
- **Как используют:**
 - Манипуляция общественным мнением.
 - Разжигание конфликтов в соцсетях.

Как защититься?

- Критически оценивать контент (проверять источники).
- Использовать двухфакторную аутентификацию.
- Обучать ИИ-системы распознавать атаки (например, анти-Deepfake-алгоритмы).

Важно: Нейросети — лишь инструмент. Риски зависят от того, в чьих руках они находятся.

Этот список можно дополнить примерами из новостей (например, случаи мошенничества с deepfake). 😊

«ТОП-5 опасностей нейросетей»:

1. Deepfake — поддельные видео.
2. ИИ-фишинг — письма «от друга».
3. Боты-provokatory — фейковые новости.
4. Взлом паролей — ИИ перебирает быстрее.
5. Утечки данных — нейросети анализируют соцсети.

Группа 4. Пропагандисты

Ответ нейросети DeepSeek

Примеры советов:

- 📞 **Не верь неожиданным звонкам** — даже если голос звучит как родственник, перезвони ему сам.
- 🚫 **Не переходи по подозрительным ссылкам** — нейросети создают фейковые сайты-«клоны».
- 🗣️ **Проверяй странные сообщения** — спроси у человека лично, писал ли он это.

Ответ нейросети Qwen 2.5 MAX

Вот простые советы, как защититься от мошенников, которые используют нейросети.

1. Не доверяйте всему, что выглядит правдоподобно. Мошенники могут использовать нейросети, создавать фальшивые тексты, голосовые сообщения или даже видео. Если кто-то пишет или звонит вам с "срочной просьбой" — не торопитесь верить.

2. Не переходите по подозрительным ссылкам. Если вам приходит сообщение с ссылкой (например, в SMS, электронной почте или мессенджере), будьте осторожны. Нейросети могут создавать убедительные письма, которые выглядят как настоящие.

3. Не раскрывайте личные данные. Никому не говорите свои пароли, номера банковских карт или коды из SMS. Даже если человек звонит и говорит, что он "из банка" или "из службы поддержки". Настоящие сотрудники никогда не спросят такие данные.

4. Будьте осторожны с голосом знакомых. Нейросети могут подделывать голоса людей. Например, вам может позвонить "родственник" и сказать, что ему срочно нужны деньги. Перезвоните на его обычный номер, чтобы убедиться, что это он.

5. Проверяйте фото и видео. Сейчас нейросети могут создавать реалистичные поддельные фото и видео. Если вы видите что-то странное или слишком хорошее, чтобы быть правдой, найдите дополнительную информацию или спросите экспертов.

6. Используйте надежные пароли. Придумайте сложные пароли для своих аккаунтов (лучше всего комбинировать буквы, цифры и символы). Нейросети могут взламывать простые пароли, поэтому важно сделать их безопасными.

7. Будьте особенно внимательны к "срочным" просьбам. Мошенники любят создавать панику: "Срочно переведите деньги!", "Ваш аккаунт заблокирован!", "Вы выиграли, но нужно оплатить налог!".

8. Не стесняйтесь задавать вопросы. Если кто-то просит у вас деньги или данные, задавайте много вопросов. Например: "Почему вы звоните?", "Как я могу проверить, что вы настоящий сотрудник?". Мошенники обычно не любят отвечать на сложные вопросы.

9. Знайте свои права. Помните, что вы имеете право отказаться от любого предложения, даже если оно кажется заманчивым. Никто не может заставить вас что-то делать, если вы не уверены.

10. Будьте бдительны в интернете. В интернете можно встретить много мошенников, которые используют нейросети для создания фальшивых сайтов, профилей или объявлений. Всегда проверяйте, с кем вы общаетесь, и не торопитесь доверять незнакомцам.

Главное правило:

Если что-то кажется странным или вызывает сомнения — не торопитесь действовать. Лучше перепроверить, чем стать жертвой мошенников. Помните: ваша осторожность — ваша главная защита!

Будьте внимательны, и всё будет хорошо! 😊

Группа 5. Диагностики

Ответ нейросети DeepSeek

Тест по теме: "Уязвимость информационной инфраструктуры и кибербезопасность"

1. Что такое уязвимость информационной инфраструктуры?

- a) Программа для защиты от вирусов
- b) Свойство инфраструктуры, позволяющее реализовать угрозу**
- c) Метод шифрования данных
- d) Автоматизированная система мониторинга

2. Как называется умышленное воздействие на информационную инфраструктуру с помощью программных средств?

- a) Фишинг
- b) Кибератака**
- c) Шифрование
- d) Даунгрейд

3. Какой вид кибератаки направлен на перегрузку системы и отказ в обслуживании?

- a) Фишинг
- b) Вирусная атака
- c) DDoS-атака**
- d) SQL-инъекция

4. Какой фактор считается самым уязвимым в кибербезопасности?

- a) Устаревшее программное обеспечение
- b) Человеческий фактор (поведение пользователей)**
- c) Недостаточная мощность серверов
- d) Отсутствие брандмауэра

5. Какой процент кибератак на банки совершают их собственные сотрудники?

- a) 25%
- b) 50%
- c) 91%**
- d) 10%

6. Что такое эксплойт?

- a) Антивирусная программа
- b) Вредоносный код, использующий уязвимость программы**
- c) Метод шифрования данных
- d) Система резервного копирования

7. Какой термин описывает способность инфраструктуры быстро восстанавливаться после атак?

- a) Киберзащита
- b) Криптография
- c) Киберустойчивость**
- d) Файрволинг

8. Какой метод чаще всего используют злоумышленники для получения конфиденциальной информации?

- a) Физический взлом серверов
- b) Социальная инженерия (психологическое манипулирование)**
- c) Установка дополнительных антивирусов
- d) Отключение электропитания

9. Какова основная цель большинства кибератак?

- a) Развлечение
- b) Получение финансовой выгоды**
- c) Улучшение работы системы
- d) Тестирование защиты

10. Какая из перечисленных мер НЕ относится к кибербезопасности?

- a) Обновление ПО
- b) Обучение пользователей
- c) Отключение интернета навсегда**
- d) Использование антивирусов

Ключ: 1(b), 2(b), 3(c), 4(b), 5(c), 6(b), 7(c), 8(b), 9(b), 10(c)

Формат:

- 10 вопросов с 4 вариантами ответов.
- Правильные ответы выделены **зеленым**.
- Можно использовать для проверки знаний после урока или как домашнее задание.

Группа 6. Программисты

Ответ ВЛАСКВОХАИ, откорректированный учащимися

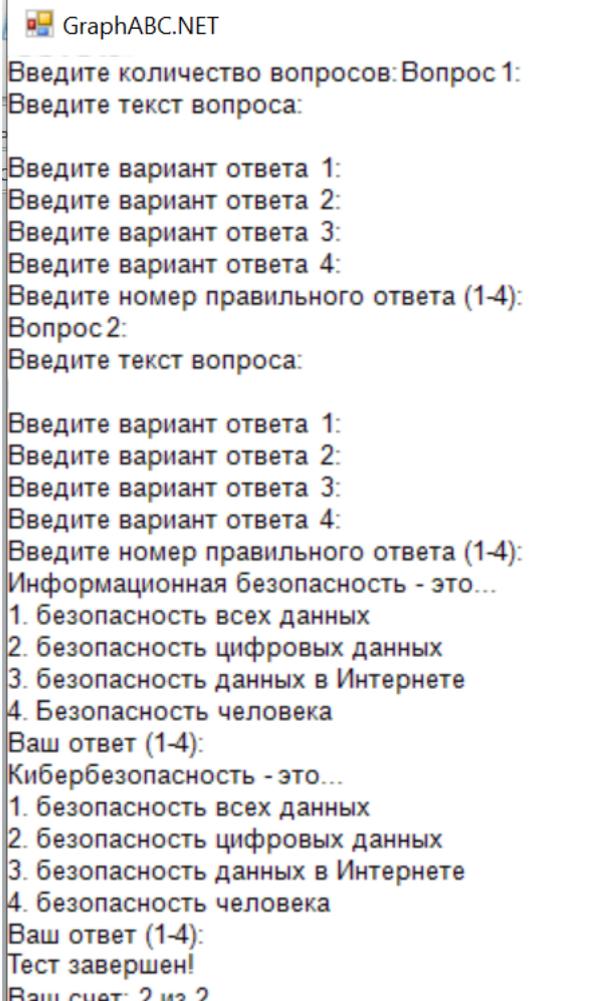
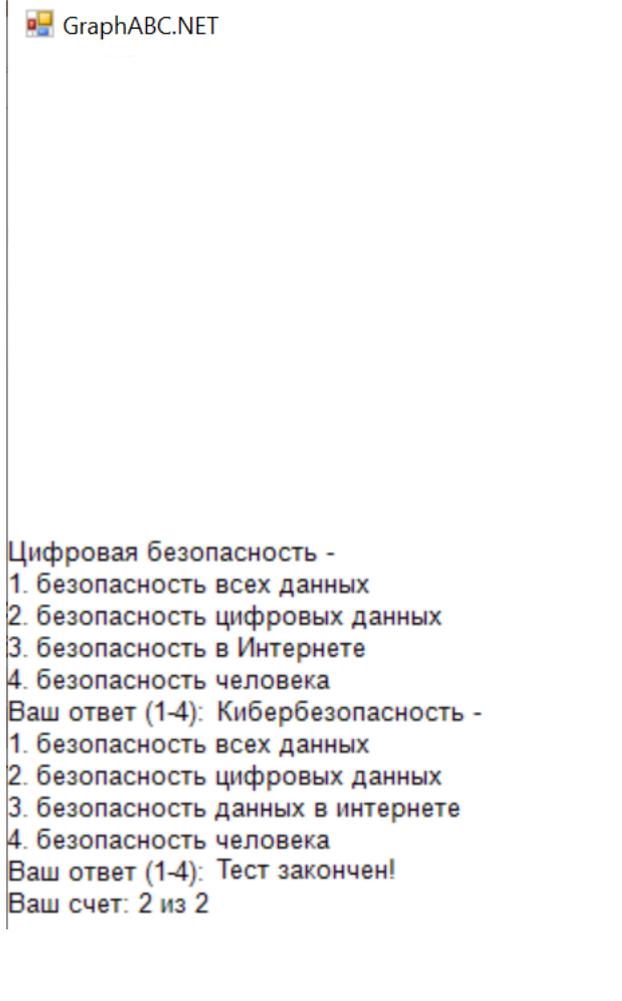
```
program TestProgram;
uses GraphABC;
type TQuestion = record
    Text: string;
    Options: array[1..4] of string;
    CorrectAnswer: integer;
end;
var Questions: array of TQuestion;
    NumberOfQuestions, UserAnswer, Score: integer;
procedure InputQuestions;
begin
    Writeln('Введите количество вопросов: ');
    ReadLn(NumberOfQuestions);
    SetLength(Questions, NumberOfQuestions);
    for var i := 0 to NumberOfQuestions - 1 do
        begin
            ClearWindow;
            WriteLn('Вопрос ', i + 1, ':');
            Writeln('Введите текст вопроса: ');
            ReadLn(Questions[i].Text);
            for var j := 1 to 4 do
                begin
                    Writeln('Введите вариант ответа ', j, ': ');
                    ReadLn(Questions[i].Options[j]);
                end;
            Writeln('Введите номер правильного варианта (1-4): ');
            ReadLn(Questions[i].CorrectAnswer);
            while (Questions[i].CorrectAnswer < 1) or (Questions[i].CorrectAnswer > 4) do
                begin
                    Writeln('Неверный ввод. Введите номер правильного ответа (1-4): ');
                    ReadLn(Questions[i].CorrectAnswer);
                end;
            end;
        end;
end;
procedure RunTest;
begin
    Score := 0;
    for var i := 0 to NumberOfQuestions - 1 do
        begin
            Writeln(Questions[i].Text);
            for var j := 1 to 4 do
                begin
                    Writeln(j, ' ', Questions[i].Options[j]);
                end;
            Write('Ваш ответ (1-4): ');
            ReadLn(UserAnswer);
            while (UserAnswer < 1) or (UserAnswer > 4) do
                begin
                    Writeln('Неверный ввод. Ваш ответ (1-4): ');
                    ReadLn(UserAnswer);
                end;
            if UserAnswer = Questions[i].CorrectAnswer then
                begin
```

```

    Inc(Score);
    end;
end;
end;
end;
procedure DisplayResult;
begin
    WriteLn('Тест закончен!');
    WriteLn('Ваш счет: ', Score, ' из ', NumberOfQuestions);
end;

begin
    InputQuestions;
    ClearWindow;
    RunTest;
    DisplayResult;
end.

```

Окно составленной нейросетью программы в процессе	Окно откорректированной учащимися программы в процессе
 <p>GraphABC.NET</p> <p>Введите количество вопросов: Вопрос 1: Введите текст вопроса: : Введите вариант ответа 1: Введите вариант ответа 2: Введите вариант ответа 3: Введите вариант ответа 4: Введите номер правильного ответа (1-4): Вопрос 2: Введите текст вопроса: : Введите вариант ответа 1: Введите вариант ответа 2: Введите вариант ответа 3: Введите вариант ответа 4: Введите номер правильного ответа (1-4): Информационная безопасность - это... 1. безопасность всех данных 2. безопасность цифровых данных 3. безопасность данных в Интернете 4. Безопасность человека Ваш ответ (1-4): Кибербезопасность - это... 1. безопасность всех данных 2. безопасность цифровых данных 3. безопасность данных в Интернете 4. безопасность человека Ваш ответ (1-4): Тест завершен! Ваш счет: 2 из 2</p>	 <p>GraphABC.NET</p> <p>Цифровая безопасность - 1. безопасность всех данных 2. безопасность цифровых данных 3. безопасность в Интернете 4. безопасность человека Ваш ответ (1-4): Кибербезопасность - 1. безопасность всех данных 2. безопасность цифровых данных 3. безопасность данных в интернете 4. безопасность человека Ваш ответ (1-4): Тест закончен! Ваш счет: 2 из 2</p>
<p>Недостатком составленной нейросетью программы является только то, что ввод вопросов теста и ответов на него осуществляется последовательно без очистки экрана.</p>	<p>Группа может откорректировать данную проблему (введя команду ClearWindow;).</p>

Опасности	Пути предотвращения
<p>Генерация фейков (Deepfake) Поддельные видео/аудио для мошенничества, клеветы</p>	<ul style="list-style-type: none"> - Использование цифровых водяных знаков. - Обучение людей проверять источники.
<p>Фишинг с ИИ Персонализированные письма/сообщения от «друзей» или «банков»</p>	<ul style="list-style-type: none"> - Включение двухфакторной аутентификации. - Проверка URL перед переходом. - Использование антифишинговых расширений (например, MetaCert).
<p>Взлом паролей Нейросети подбирают пароли в 100 раз быстрее</p>	<ul style="list-style-type: none"> - Создание сложных паролей (12+ символов, цифры, спецзнаки). - Использование менеджеров паролей.
<p>Массовый троллинг/пропаганда Боты распространяют фейковые новости, разжигают конфликты</p>	<ul style="list-style-type: none"> - Модерация соцсетей с помощью ИИ. - Отчеты пользователей о подозрительных аккаунтах.
<p>Кража личных данных Нейросети анализируют соцсети для шантажа или мошенничества</p>	<ul style="list-style-type: none"> - Ограничение доступа к личным данным в соцсетях. - Использование виртуальных номеров для регистраций.
<p>Автоматизация кибератак ИИ-вирусы, адаптирующиеся к защите</p>	<ul style="list-style-type: none"> - Регулярное обновление ПО. - Установка антивирусов с ИИ (например, Darktrace).
<p>Мошенничество в финансах Фейковые инвестиционные советы, поддельные голосовые звонки «от банка»</p>	<ul style="list-style-type: none"> - Проверка официальных источников перед переводом денег. - Обучение сотрудников банков распознаванию ИИ-мошенничества.