ГБОУ СОШ № 10
государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа № 10
имени полного кавалера ордена Славы Петра Георгиевича Макарова
города Жигулевска городского округа Жигулевск Самарской области

445359, Российская Федерация, Самарская область, городской округ Жигулевск, город Жигулевск, В-1, д. 29. Телефон/факс: 8 (848-62) 2-54-40. E-mail: cu_sch10zhg@63edu.ru

ПРОВЕРЕНО
заместитель директора по ВР
Е.Н. Клопова

УТВЕРЖДЕНО
Директор ГБОУ СОШ № 10
Е.А. Шер
Приказ № 110/5-од
от « 31 » августа 2026 г



C=RU, O=ГБОУ СОШ № 10,
CN=Е.А. Шер,
E=cu_sch10zhg@63edu.ru
2026.08.31 13:33:19+04'00'

РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ и ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
5-9 классы

Пояснительная записка

Программа курса внеурочной деятельности «Искусственный интеллект и информационная безопасность» интегрирует знания различных учебных предметов, направлена на формирование межпредметных связей с информатикой, развитие компетенций обучающихся в области современных информационных и коммуникационных технологий (ИКТ), основанных на достижениях науки и IT-отрасли. Программа способствует формированию технологической грамотности обучающихся и актуального для информационного общества мышления, развитию навыков работы с технологиями искусственного интеллекта (далее – ИИ), умений эффективно их использовать, свободно ориентироваться в цифровой среде и ответственно вести себя в ней с точки зрения информационной безопасности (далее – ИБ).

Содержание программы выстроено вокруг сквозной идеи: совет дает ИИ, а решение и ответственность остаются за человеком. На уровне 5-7 классов обучающиеся знакомятся с понятием искусственного интеллекта и базовыми правилами безопасного поведения в цифровой среде. На уровне 8-9 классов эти представления углубляются и связываются с содержанием курса информатики основного общего образования (измерение и представление информации, логические основы, алгоритмизация и программирование, моделирование, управление и обратная связь), что позволяет раскрыть, как устроены технологии ИИ и какие угрозы информации они создают и одновременно помогают отражать.

Программа курса «Искусственный интеллект и информационная безопасность» ориентирована на:

– приоритеты и перспективы, обозначенные в Стратегии научно-технологического развития Российской Федерации (утверждена Указом Президента РФ от 28.02.2024 № 145 «О Стратегии научно-технологического развития Российской Федерации»);

– требования информационного общества, инновационной экономики и научно-технологического развития;

– Национальную стратегию развития искусственного интеллекта на период до 2030 года (утверждена Указом Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации»);

– федеральный проект «Искусственный интеллект», входящий в национальный проект «Экономика данных и цифровая трансформация государства».

В ходе освоения программы происходит совершенствование цифровых навыков обучающихся, что является не только базовым требованием для интеграции человека в современный информационный мир, но и необходимым условием успешной учебы и работы, возможностью приобрести востребованную специальность и иметь преимущество на рынке труда.

Программа знакомит обучающихся с понятием и сущностью искусственного интеллекта, историей его создания и развития, преимуществами и рисками, связанными с использованием ИИ, сферами и способами применения ИИ-технологий, перспективами их использования. Рядом с линией ИИ проходит линия информационной безопасности: обучающиеся рассматривают персональные данные и цифровой след, пароли и аутентификацию, социальную инженерию и онлайн-мошенничество, вредоносное программное обеспечение и средства защиты, достоверность информации и дипфейки, этические нормы использования ИИ. Обучающиеся получат навыки работы с искусственным интеллектом, в том числе быстрого решения учебных задач и познания нового, научатся генерировать тексты и изображения, сочинять музыку, а также применять изученные правила для защиты себя и своей информации в цифровой среде. Обучающиеся познакомятся с возможностями использования ИИ для анализа и проверки отдельных этапов учебной работы, уточнения объяснений и самопроверки в пределах, определенных педагогом, при обязательном сохранении самостоятельного выполнения основных познавательных действий.

Программа конкретизирует содержание, планируемые предметные, метапредметные и личностные результаты. Стратегическими документами, определяющими содержание и результаты обучения, являются федеральный государственный образовательный стандарт основного общего образования, утверждённый приказом Минпросвещения России от 31.05.2021 № 287 и от 18.06.2025 № 467 и соответствующая федеральная образовательная программа основного общего образования, утверждённая приказом Минпросвещения России от 18.05.2023 № 370.

Основной целью освоения содержания программы является получение обучающимися знаний, умений и навыков в области искусственного интеллекта и информационной безопасности; критического отношения к информации; коммуникации в цифровом пространстве в условиях обеспечения информационной безопасности; воспитания ответственного отношения к воспринимаемой информации с учетом этических норм ее использования и распространения, стремления к продолжению образования в области искусственного интеллекта и продуктивной деятельности с применением технологий ИИ.

Задачами курса являются:

- овладение знаниями об основах искусственного интеллекта и его применении в современном мире, технологиях искусственного интеллекта, вызовах и ограничениях искусственного интеллекта, этических вопросах, связанных с его развитием и использованием;
- формирование представлений об информационной безопасности и умений защищаться от мошеннических действий, в том числе совершаемых с применением технологий искусственного интеллекта;
- формирование умений обоснованно и ограниченно использовать разрешенные педагогом инструменты ИИ для отдельных учебных действий с обязательной проверкой результата;
- формирование умений пользоваться сервисами для синтеза речи, генерировать тексты и изображения с помощью искусственного интеллекта, выполнять учебные задачи с опорой на инструменты ИИ;
- овладение умениями работать с различными видами информации, самостоятельно планировать и осуществлять индивидуальную и коллективную информационную деятельность, представлять и оценивать ее результаты;
- формирование последовательного, логичного и критического мышления как необходимого условия профессиональной деятельности в современном высокотехнологичном обществе;
- формирование цифровых навыков, в том числе ключевых компетенций взаимодействия с цифровыми средами, основы работы с данными, коммуникация на современных цифровых платформах, информационная безопасность; воспитание критического отношения к информации с учетом правовых и этических норм ее использования, распространения и генерирования.

Образование обучающихся в сфере искусственного интеллекта и информационной безопасности носит интегративный характер; способствует развитию интереса к учебно-познавательной деятельности, основанной на практической включенности в различные ее виды, в том числе социальную, трудовую, игровую, исследовательскую и проектную; знакомит обучающихся с перспективным направлением учебной и профессиональной деятельности; создает условия для личностного роста и профессионального самоопределения в соответствии со своими возможностями, способностями и с учетом требований рынка труда и приоритетов государственного развития. Реализация программы призвана способствовать формированию технологически грамотного и ответственного школьника при сохранении ведущей роли педагога, живого общения и самостоятельной познавательной

деятельности.

Занятия по программе курса проводятся 1 академический час в неделю для каждого класса в течение всего учебного года в форме, отличной от урочной (игры, викторины, квесты, разбор кейсов, тренажеры и др.).

Использование инструментов ИИ осуществляется в педагогически обоснованных случаях под контролем учителя. Педагог определяет цель, содержание, продолжительность и допустимый формат работы, предварительно оценивает используемые сервисы и материалы, организует обсуждение и проверку результатов. Основные объясняющие, воспитательные и оценочные функции осуществляются педагогом; самостоятельная работа обучающегося является обязательным условием выполнения задания.

Программа курса «Искусственный интеллект и информационная безопасность» реализуется в рамках внеурочной деятельности и соотносится с целями и задачами Единой модели профориентации. Курс дополняет профориентационный курс «Россия – мои горизонты» в части знакомства с профессиями на стыке искусственного интеллекта и информационной безопасности, формирования представлений о требованиях к специалистам и траекториях профессионального входа, сопоставления задач профессии с востребованными школьными знаниями и планирования личной образовательной траектории с учётом требований ОГЭ и профильных учебных предметов. Эта линия выстроена от отдельных занятий, показывающих, где и как применяется ИИ, к специальному занятию «Кем быть: профессии, где нужен искусственный интеллект», и закреплена в личностных результатах в виде интереса к практическому изучению профессий в сфере ИИ и осознания их перспективности для определения жизненных траекторий.

Содержание курса внеурочной деятельности
«Искусственный интеллект и информационная безопасность»

5-7 КЛАССЫ

Занятие 1. Искусственный интеллект и как с ним общаться безопасно

ИИ решает задачи, которые раньше умел решать только человек: распознаёт лица и голос, генерирует тексты и изображения, решает игровые задачи. Чем ИИ отличается от человека? Мифы и реальность. Главное правило безопасности при общении с ИИ – совет дает ИИ, а решает человек. ИИ не может заменить родителей, друзей или психолога. Риск доверительных отношений ИИ.

Занятие 2. Эволюция нейросетей и информационная безопасность

Как возникала идея технологии, которая «думает»: от первых программ и шахмат до голосовых помощников и ИИ-агентов. Приоритет развития отечественных технологий ИИ.

Риски применения ИИ: чем умнее технология, тем важнее уметь пользоваться ею безопасно. Что такое информация и почему ее боятся потерять. Простое правило: информацию можно создать, передать, потерять или украсть. Какую информацию нельзя доверять нейросети.

Занятие 3. Вклад российских ученых в развитие искусственного интеллекта

Как ИИ помогает ученым делать открытия: быстрый перебор вариантов, поиск закономерностей в больших данных, предсказывание свойств веществ и др.

Российские ученые, исследования которых стали основанием для возникновения ИИ и способствовали его развитию, например: М.А. Бурцев, В.Н. Вапник, А.И. Галушкин, А.В. Гасников, В.М. Глушков, А.Н. Колмогоров, С.И. Корсаков, А.А. Ляпунов, Ю.Е. Нестеров, Д.А. Поспелов, А.Я. Червоненкис и др.

Занятие 4. Как мы думаем и как «думает» компьютер: про нейроны и нейросети

Думать, запоминать и решать задачи помогает головной мозг: он собирает ощущения, сравнивает с прошлым опытом и выбирает действие. Головной мозг и нейроны. Как много нейронов вместе умеют учиться. Почему современная нейросеть подсказана устройством головного мозга, но «думает» по-другому? Чтобы быть в безопасности, нужно уметь распознать, рассуждает ли человек или ИИ вместо него.

Занятие 5. Правда или выдумка: учимся проверять информацию

Отличие факта от мнения. Признаки ложной и подозрительной публикации. Как проверить источник и сравнить его с другим. ИИ тоже генерирует недостоверные факты, поэтому проверять надо и его ответы. На сколько важно содержание ответов ИИ с точки зрения культуры и мировоззрения: какие оценки включены в текст ответа, какие обстоятельства опущены, как выбор слов влияет на восприятие события.

Занятие 6. Фантастика в прошлом – реальность в настоящем

Как писатели, режиссеры и художники представляли умные машины и что из этих мечтаний сбылось. ИИ в литературе, кино и живописи. Где мечта стала настоящей технологией. Почему «злой робот из кино» – это не настоящая опасность, а использование ИИ в реальности влечет угрозы, которые нужно уметь узнавать.

Занятие 7. Этика и мораль для искусственного интеллекта

Что такое этика и мораль ИИ: правила, которым компьютер учат люди. Настоящее и будущее ИИ. Право и защита человека от злоупотреблений ИИ, главное правило – «решает человек». Нравственная оценка поступка осуществляется человеком, а ответ модели не обладает самостоятельным моральным авторитетом. Допустимо ли создавать изображение одноклассника, которое может его задеть или обидеть. Можно ли сгенерировать поздравление и представить его как собственное искреннее обращение. Как поступить, если предложенный сервисом ИИ текст содержит оскорбительные обобщения.

Занятие 8. Обманывать в сети тоже плохо. Обман на доверии

Злоумышленник чаще всего обманывает не технику, а человека: торопит, пугает или льстит, чтобы выманить данные и пароли. Признаки манипуляции в переписке и по телефону. Признаки вербовки детей. Алгоритм действий в случае вербовки: не выполнять «поручения» незнакомцев в интернете, сообщить родителям или педагогу, сохранить переписку. ИИ делает обман убедительным, ведь голос и лицо «близкого» человека можно подделать.

Занятие 9. ИИ вокруг нас каждый день: телефон, навигатор, умная колонка

ИИ уже в телефоне, навигаторе, игре и умной колонке. Примеры каждый день: переводчик и проверка орфографии, рекомендации фильмов и музыки, навигатор, голосовой помощник, распознавание фото. Помощники собирают данные о нас, поэтому важно понимать, какие именно и как себя защитить.

Занятие 10. Пароль как ключ от двери: делаем его надежным

Пароль как ключ от «цифровой комнаты». Зачем нужны пароли и почему их нельзя никому сообщать, даже друзьям. Признаки надежного пароля и опасность одного пароля на все сайты. Простыми словами про менеджер паролей и двухфакторную проверку с кодом из СМС. Как злоумышленники с помощью ИИ угадывают простые пароли и подделывают голос друга. Как создать надёжный пароль на учебном аккаунте, проверить разрешения установленных приложений (камера, микрофон, геолокация). «Угон» личных аккаунтов через код из СМС.

Занятие 11. Общаемся в сети безопасно: мессенджеры и незнакомцы

Сетевой этикет, поведение в группах и игровых чатах. Действия при травле в сети: не отвечай, сохрани копии экрана, сообщи взрослым, заблокируй обидчика. Правило обращения к родителям, педагогу или школьному психологу при переживании конфликта, травли (буллинга) и иных сложных жизненных ситуаций.

Опасные знакомства: виртуальный незнакомец не всегда может стать твоим другом. Иногда в онлайн-игре «другом» может оказаться робот или злоумышленник с помощью ИИ. Как с помощью ИИ ведут поиск потенциальных жертв среди детей и «передают» их злоумышленникам. Просьба включить геолокацию или уйти в личный чат – всегда повод насторожиться. Как защитить себя от опасных знакомств. Как защитить свои смартфоны.

Занятие 12. Как ИИ «видит», «слышит», «говорит»

У компьютера свои «органы чувств» (датчики и сенсоры): программа распознает лицо и текст на фото, превращает голос в текст и обратно, распознаёт речь. Почему компьютеру трудно распознать шутку или двусмысленность. Риски «слежки» за человеком.

Занятие 13. Мои данные и цифровой след: все сохраняется надолго

Что такое персональные данные: адрес, телефон, школа, фото в социальных сетях. Почему все, попавшее в сеть, оставляет след, который почти нельзя стереть. Цифровая репутация и ответственная публикация. ИИ тоже обучается на наших данных и по ним распознаёт людей, поэтому личные данные нужно беречь. Правилами обращения с данными при выполнении учебных заданий.

Занятие 14. Кто собирает мои данные: настройки и согласия сайтов

Как сайты и приложения собирают данные и зачем это. Настройки приватности и геолокация. Почему просят «подтвердить возраст картой» и что в этом опасного. Учимся беречь приватность и читать простые правила согласия. Как собранные данные питают ИИ-рекомендации и влияют на то,

что нам показывают. Как ИИ-системы круглосуточно анализируют потоки публичной информации в поисках «жертв» для мошенничества.

Занятие 15. «Умный» дом и «умный» город: как техника заботится о нас

Умные устройства собирают данные с датчиков в квартире или целом городе, анализируют их и сами принимают полезные решения про регулирование освещения, отопления и движения транспорта. ИИ в отечественном транспорте (умные поезда, авионика) и городской среде (системы безопасный город, распознавание номеров). Как в городе, который все измеряет и собирает данные о людях, стирается граница приватности.

Занятие 16. Цифровые двойники: точная копия для опытов без вреда

Цифровой двойник – это виртуальная копия реального объекта (машины, здания, человека), на которой можно пробовать и ошибаться без вреда для настоящего. Но данные двойника чувствительны, и копия может быть использована против оригинала. Цифровой двойник самолета или завода: как инженеры тестируют новые детали в виртуальном мире.

Занятие 17. Подделка и обман: как ИИ создает фейки и как их узнать

ИИ создаёт похожие на правду синтетические подделки: поддельные видео, записи голоса, сообщения для обмана. Признаки подделки. ИИ помогает и мошенникам, и защитникам. Самопроверка: «кто это сделал?» и «откуда это?»; не сообщать код из СМС даже «другу». Всегда нужно помнить про защиту от дезинформации и обмана голосом и лицом.

Занятие 18. Ловушки в сети: как распознать мошенника

Приманка всегда выглядит заманчиво или страшно, ее цель вывести из безопасного интернет-пространства. Подозрительные письма и ссылки (письма-приманки), фальшивые подарки, конкурсы и «легкие деньги». Бесплатные игровые ресурсы как приманка, переход из игрового чата в мессенджер как сигнал опасности, просьба сфотографировать экран телефона родителя как верный признак мошенничества, таймер обратного отсчёта как приём психологического давления. Современные приманки ИИ еще убедительнее. Что делать, если обман уже произошел? Простые правила (позвонить 102 или 112, сообщить родителям, не удалять переписку, не переводить деньги).

Занятие 19. Учусь честно: нейросеть мне помогает, а не делает работу за меня

Нейросеть – это советчик и тренажер, а не тот, кто делает твою работу. Как запросить у ИИ разбор непонятного и сгенерировать вопросы для самопроверки. Риски привычки немедленно обращаться к ИИ при любом

затруднении. Правила честности: сначала подумай сам, потом сверься; проверяй факты; называй источник; не выдавай чужое и результат генерации ИИ за свое; обязательно проверяй ответы ИИ на ошибки.

Занятие 20. ИИ рисует и сочиняет: кто здесь автор

ИИ рисует, сочиняет тексты и мелодии по заданию человека, но замысел и выбор остаются за человеком. Как рождается картинка или текст по описанию? Надо ли отмечать то, что сделано с помощью ИИ. Как соблюдаются авторские права. Честное и ответственное использование ИИ.

Занятие 21. ИИ на страже здоровья: границы доверия

Что замечает человек, что выявляет ИИ, и почему им лучше работать вместе. Как ИИ помогает врачу обнаружить то, что тот может не заметить. Как ИИ помогает следить за здоровьем: анализирует показатели спортивных браслетов и датчиков, рентгеновские снимки и кардиограммы. Самолечение по совету ИИ опасно. Данные гаджета доступны не только владельцу: безопасность передачи и хранения, настройка доступа.

Занятие 22. Безопасность финансовых средств в цифровой среде

Онлайн-банкинг и банковские приложения. Системы для защиты платежей и данных клиентов от злоумышленников. Голосовая биометрия. Типовые схемы атак на семейный бюджет.

Занятие 23. Почему «заболел» компьютер: вредоносные программы

Вирусы и опасные файлы приходят незаметно. Почему нельзя скачивать и открывать файлы из непроверенных источников. Безопасная загрузка программ и роль антивируса. ИИ помогает антивирусам узнавать новые вирусы, но и мошенникам помогает их прятать.

Занятие 24. ИИ на заводе и в поле: быстрее, больше, лучше

На заводах ИИ нужен, чтобы делать быстрее, больше и качественнее: робот-сборщик и проверка деталей на брак, умное сельское хозяйство и транспорт. Беспилотная техника в сельском хозяйстве и на закрытых территориях. Что будет с людьми: часть работы берет ИИ, часть остается за человеком. Почему за важные решения до сих пор отвечает человек. Чем «умнее» производство, тем больше оно подвержено информационным атакам. Поэтому его нужно защищать.

Занятие 25. Искусственный интеллект и информационная безопасность в космосе

Как ИИ помогает осваивать космос, распознавать снимки Земли и данные дистанционного зондирования, планировать научные миссии, искать внеземные сигналы. Космические системы связи. Передача данных между Землей и космосом: какие могут быть угрозы.

Занятие 26. Кем быть: профессии, где нужен искусственный интеллект

Какие профессии связаны с ИИ и данными: кто обучает ИИ, проверяет и защищает их. Какие навыки пригодятся в этих и других профессиях. Одна из самых нужных профессий – специалист по кибербезопасности.

Занятие 27. Я, нейросеть и моя безопасность: итоговый разговор

Возвращаемся к пройденному пути и собираем личный «паспорт безопасности». Подводим итоги: «ИИ это…», «он умеет…», «в нем нельзя…», «как я себя берегу». Закрепляем правило: совет дает ИИ, решает человек.

8-9 КЛАССЫ

Занятие 1. Искусственный интеллект: какие задачи он решает и где ошибается

Задачи, которые ИИ решает на уровне человека: распознавание образов и речи, генерация текста и изображений, планирование, игра. Отличие обучаемой модели ИИ от обычной программы: результат формируется на основе данных, а не задается жесткой инструкцией. Границы применимости: почему модель ИИ, хорошо решающая одну задачу, беспомощна в другой. Ключевое правило: совет дает ИИ, а решение и ответственность – за человеком.

Занятие 2. Эволюция идей искусственного интеллекта: от логических правил к обучению на данных

Основные этапы развития ИИ: символический ИИ и экспертные системы, статистическое обучение, генеративные алгоритмы в составе обученных моделей и ИИ-агенты. Роль накопления данных и роста вычислительных мощностей. Роль контроля человека, проверяемость результатов работы генеративного ИИ, защита обрабатываемой информации.

Приоритет развития отечественной микроэлектроники и центров обработки данных.

Занятие 3. Вклад отечественных ученых в развитие искусственного интеллекта

Как ИИ помогает науке делать открытия: быстрый перебор вариантов, поиск закономерностей в больших данных, предсказание свойств веществ, обработка результатов наблюдений. Ученые, чьи работы стали основанием для возникновения ИИ и способствовали его развитию, например: М.А. Бурцев, В.Н. Вапник, А.И. Галушкин, А.В. Гасников, В.М. Глушков, А.Н. Колмогоров, С.И. Корсаков, А.А. Ляпунов, Ю.Е. Нестеров, Д.А. Поспелов, А.Я. Червоненкис и др. Дискуссия о кибернетике в СССР, становление отечественной вычислительной техники и школы машинного перевода текста.

Занятие 4. Как устроена искусственная нейронная сеть: от формального нейрона к обучаемой модели

Мозг и нейрон как источник аналогии, но не копия: математическая модель нейрона. Почему сеть с миллионами параметров не «понимает» текст: статистический характер вывода. Умение отличить рассуждение человека от ответа ИИ и формулировать уточняющие запросы.

Занятие 5. Достоверность информации и методы ее проверки: факт, оценка, источник

Разграничение факта, оценки и мнения. Критерии достоверности и актуальности. Перекрестная проверка источника и работа с первичными публикациями. Культурное и мировоззренческое содержание ответов ИИ. Признаки сфабрикованной и манипулятивной информации. Проверка изображений, ссылок и метаданных. ИИ уверенно генерирует правдоподобные ошибки («галлюцинации»), поэтому ответ нейросети требует такой же проверки, как и любой внешний источник.

Занятие 6. От научной фантастики к инженерии: какими представляли умные машины и что стало технологией

Образ «думающей машины» в литературе, кинематографе и изобразительном искусстве: от автоматов и роботов К. Чапека и А. Азимова до современных языковых моделей. Какие прогнозы сбылись, а какие остались метафорой и почему. «Восставший робот» – сюжетный прием. Реальные риски связаны со злоупотреблением технологиями: слежкой, дезинформацией, манипуляцией и утратой контроля. Умение узнавать настоящие угрозы.

Занятие 7. Этика и правовое регулирование искусственного интеллекта

Этические принципы ИИ: справедливость, прозрачность, объяснимость, безопасность, подотчетность. Права человека в среде ИИ-сервисов: защита от дискриминации алгоритмами, право на объяснение, принцип «человек принимает решение».

Занятие 8. Социальная инженерия: как обманывают не компьютер, а человека

Психологические приемы: дефицит времени, страх, лесть, авторитет, жадность. Типовые сценарии: ложная служба поддержки, розыгрыш, «помощь знакомого», «срочная оплата».

Вербовка подростков в качестве «дропперов» и «воркеров» через онлайн-игры и социальные сети, «работа курьером», ложные сообщения о минировании по заданию куратора, вербовка в мессенджерах. «Несложные поручения» в интернете как вовлечение в уголовно наказуемую деятельность: «работа курьером» или «приём и перевод денег на карту» может быть квалифицирована как соучастие в мошенничестве (статья 159 УК РФ), пособничество в терроризме (статья 205.1 УК РФ) или участие в организованном преступном сообществе (статья 210 УК РФ), а попытки «подработки» в теневом сегменте интернета – как создание или использование вредоносных программ (статья 273 УК РФ) или неправомерный доступ к компьютерной информации (статья 272 УК РФ).

Как ИИ усиливает манипуляцию: голос и лицо «близкого» человека можно подделать, текст – сгенерировать без ошибок, приманку – персонализировать. Личный алгоритм: пауза, проверка по независимому каналу, отказ называть код и персональные данные, обращение к взрослому или в поддержку сервиса.

Занятие 9. ИИ в повседневных цифровых сервисах: принципы работы, настройки, приватность

Как устроены привычные сервисы: поисковая выдача и рекомендации, переводчики, распознавание речи, автодополнение, навигация, голосовые помощники. Понятие обучаемой модели и ее зависимости от данных пользователя. Какие данные собирают о нас сервисы и как ограничить это настройками приватности и разрешениями приложений.

Занятие 10. Аутентификация и защита доступа

Пароль как ключ доступа. Связь между длиной пароля, мощностью используемого алфавита и количеством возможных комбинаций. Менеджеры паролей, двухфакторная аутентификация, одноразовые коды. Биометрия и аппаратные ключи (токены) как основа защиты. Уникальность пароля для каждого сервиса. Как настроить двухфакторную аутентификацию, осуществить проверку утечек паролей через открытые сервисы, провести аудит cookie и трекеров в браузере. «Угон» личных аккаунтов через код из СМС. Как ИИ помогает атакующим: автоматический подбор по словарям и базам утечек, подделка голоса знакомого.

Занятие 11. Безопасное общение в цифровой среде: сетевой этикет, анонимность, верификация собеседника

Сетевой этикет и поведение в учебных и игровых сообществах. Кибербуллинг и способы противодействия. Что делать, если тебя травят в сети (не отвечать, сохранить скриншоты, сообщить взрослым, заблокировать обидчика). Что делать, если ты свидетель травли (не присоединяться, сообщить). Правовые последствия травли и распространения личной информации (статьи 128.1, 137 УК РФ). Контакты горячих линий. Принцип «по другую сторону экрана может быть и человек, и ИИ-агент»: верификация собеседника в переписке и голосовом чате. Как с помощью ИИ ведут поиск потенциальных жертв среди детей и «передают» их злоумышленникам. Признаки опасных знакомств: уход в личный чат, просьба включить геолокацию, уговоры о деньгах и данных. Защита своего устройства и аккаунтов.

Занятие 12. Компьютерное распознавание изображений, речи и текста: признаки, модели, ошибки

Как компьютер «видит» с помощью датчиков и сенсоров: дискретное представление изображений и звука (пиксель, цветовая модель). Распознавание речи и синтез голоса, оптическое распознавание текста, компьютерное зрение, генерация изображений по описанию. Трудности распознавания: двусмысленность, ирония, шум в данных. Риск слежки и этические ограничения работы с биометрией.

Занятие 13. Персональные данные, цифровой след и цифровая репутация

Что относится к персональным данным и как они защищаются. Права субъекта данных. Цифровой след: cookie, метаданные переписки, публикации, геолокация. Как ИИ связывает разрозненные данные в профиль и находит человека по косвенным признакам. Управление цифровой репутацией: что публиковать безопасно, как ограничивать сбор и удалять данные. Правилами обращения с данными при выполнении учебных заданий.

Занятие 14. Согласия, настройки приватности и профилирование: кто и как собирает данные

Пользовательские соглашения, политики конфиденциальности, cookie-уведомления: как читать и что искать. Разрешения приложений: геолокация, микрофон, камера, контакты. Профилирование и персонализация рекламы. Как собранные данные питают ИИ-рекомендации и влияют на то, что нам показывают. Как ИИ-системы круглосуточно анализируют потоки публичной информации в поисках жертв для мошенничества.

Занятие 15. Промышленный и бытовой интернет вещей в умном городе: автоматизация, обратная связь, большие данные

Интернет вещей: «бытовой» (умная лампочка) и «промышленный» (датчики на турбине или беспилотном комбайне). Сбор данных с датчиков и принятие решений: освещение, отопление, движение транспорта, видеонаблюдение. Безопасность интернета вещей: пароли по умолчанию, уязвимые прошивки, открытые сети; как защитить домашнюю сеть. Большие данные и цифровые платформы города: чем полезен анализ и где проходит граница приватности при тотальном сборе данных.

Занятие 16. Цифровые двойники

Цифровой двойник как компьютерная модель объекта, на которой можно экспериментировать без риска. Роль ИИ в калибровке и прогнозировании цифрового двойника. Риски: чувствительность данных цифрового двойника, возможность использовать копию против оригинала.

Занятие 17. Синтетические медиа: дипфейки и методы их обнаружения

Генерация реалистичных видео, аудио и изображений на основе глубоких моделей и массовое распространение поддельного контента. Признаки подделки: артефакты, несогласованность мимики, метаданные файла, водяные знаки, отсутствие подтверждения в независимых источниках. Отсутствие заметных признаков подделки не подтверждает подлинность материала. ИИ работает на обеих сторонах: и на стороне подделки, и на стороне защиты. Регламент: «не верь глазам – проверь источник, уточни у адресата напрямую, не сообщай коды».

Занятие 18. Онлайн-мошенничество: технические и социальные механизмы, действия после инцидента

Типовые схемы: фишинговые письма и ссылки, фальшивые конкурсы и «легкие деньги», поддельные службы поддержки, мошенничество с картами, бесплатные игровые ресурсы, переход из игрового чата в мессенджер, просьба сфотографировать экран телефона родителя, таймер обратного отсчёта. ИИ усиливает приманки: безупречный язык, персонализация, имитация голоса и видео, автоматизация массовых рассылок. Алгоритм действий, если обман произошел: зафиксировать доказательства, сменить пароли, сообщить взрослым, обратиться в поддержку сервиса и в полицию. Как подать заявление через электронную приёмную на сайте МВД России, что сохранить как доказательство (скриншоты с датой и временем, выписки из банковского приложения, детализация звонков), как получить талон-уведомление, Возможные последствия участия подростков в мошенничестве (статья 159 УК РФ).

Занятие 19. Нейросеть как инструмент обучения, а не замена мышлению: академическая честность

Роль ИИ в учебной работе: разобрать сложное, составить вопросы для самопроверки, проверить черновик, стать тренажером формулировок. Приемы формулирования запроса и обязательная проверка результата. Риски привычки немедленно обращаться к ИИ при любом затруднении Распознавание ошибок модели. Ссылка на источник и авторство идеи. Правила честности: сначала реши сам, потом сверься, проверяй факты, не выдавай сгенерированное ИИ и чужое за свое. «Ручная» проверка результатов работы ИИ: существование приведенных ссылок, документов, цитат и статистических данных.

Занятие 20. Генеративный ИИ и авторское право: кто автор созданного ИИ произведения

Как реализуется генерация текста, изображений и музыки: ИИ –

инструмент, а самостоятельный творческий этап, предшествующий обращению к сервису ИИ остаются за человеком. Правовой статус сгенерированного контента: авторское право, права на изображение и голос, договоры с сервисами, маркировка ИИ-контента. Этика использования: отмечать работу, выполненную с ИИ, и ответственное отношение к труду.

Занятие 21. ИИ на службе медицины: задачи диагностики, ограничения, ответственность

Компьютерное распознавание медицинских изображений и сигналов: снимки, кардиограммы. Почему ИИ эффективен как «второй взгляд», но не заменяет врача. Постановка диагноза и забота о пациенте – ответственность врача. Опасность самолечения. Как фитнес-устройства собирают и анализируют показатели и на их основе строят рекомендации: безопасность передачи медицинских данных и их хранение, настройка доступа.

Занятие 22. Безопасность финансовых средств в цифровой среде

Онлайн-банкинг и мобильные приложения: реквизиты карты и коды подтверждения. Системы защиты платежей и данных клиентов. Роль биометрии и её уязвимость перед подделкой голоса нейросетью. Типовые схемы атак на семейный бюджет: фальшивая служба поддержки, «замороженные» и «ошибочные» переводы, поддельные операции по карте, мошенничество с рассрочками и микрокредитами.

Занятие 23. Вредоносное программное обеспечение и современные средства защиты

Виды вредоносного ПО: вирусы, черви, трояны, шифровальщики, шпионское ПО. Пути распространения и признаки заражения. Как работает антивирус. Роль машинного обучения в обнаружении новых образцов. Обновления и резервное копирование. ИИ на стороне атакующих: генерация изменчивого кода, обход эвристики, точечные атаки. Безопасная загрузка программ. Понятие таргетированных атак на предприятия и критическую инфраструктуру (почему обычный антивирус не защитит завод).

Занятие 24. Искусственный интеллект в промышленности и сельском хозяйстве: автоматизация и безопасность

Задачи ИИ на производстве: компьютерное зрение для контроля качества, роботизированные линии, умное сельское хозяйство и транспорт. Что остается человеку: часть работы берет компьютер, ответственность за важные решения – за человеком. Чем «умнее» производство, тем оно уязвимее для информационных атак: защита критической инфраструктуры.

Занятие 25. ИИ в авиации, космосе и беспилотных системах. Защита каналов связи

Как ИИ помогает осваивать космос, распознавать снимки Земли и

данные дистанционного зондирования, планировать научные миссии, искать внеземные сигналы. Космические системы связи: канал «Земля – борт – Земля», значительная задержка сигнала и ее последствия для управления. Угрозы передачи данных между Землей и космосом: перехват сигнала, подмена команд и телеметрии, компрометация наземного сегмента.

Занятие 26. Профессии на стыке ИИ и информационной безопасности: требования и траектории

Профессии цикла данных и ИИ: кто обучает ИИ, проверяет, сопровождает и развивает. Профессии информационной безопасности: специалист по защите информации, аналитик центра мониторинга, тестировщик на проникновение. Инженерные профессии в высокотехнологичном секторе. Какие школьные знания востребованы: программирование, алгоритмизация, основы сетей и криптографии, работа с большими данными. Важность физики и инженерного мышления. Индивидуальная траектория: профильные предметы, олимпиады, ОГЭ по информатике, проекты и дополнительные курсы.

Занятие 27. Личный регламент работы с ИИ и базовые правила информационной безопасности

Собираем личный «паспорт безопасности» и регламент работы с ИИ-сервисами. Подводим итоги: «ИИ – это…», «ИИ умеет…», «в нем нельзя…», «как я себя берегу». Закрепление ключевого правила безопасного использования ИИ: совет дает ИИ, решает человек.

Планируемые результаты освоения программы
курса внеурочной деятельности
«Искусственный интеллект и информационная безопасность»

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

В результате освоения программ курса внеурочной деятельности «Искусственный интеллект и информационная безопасность» у обучающегося будут сформированы следующие личностные результаты.

1. Патриотическое воспитание:

− понимание роли науки и технологий, в том числе информационных и коммуникационных, в обеспечении устойчивого развития и будущего российского государства и общества в условиях стремительных изменений современного мира, когда первенство в исследованиях и разработках, освоении новых знаний и создании инновационной продукции является ключевым фактором, определяющим конкурентоспособность национальных экономик и эффективность национальных стратегий безопасности;

− ценностное отношение к достижениям российских ученых, инженеров, специалистов в области ИКТ; признание вклада отечественной научной школы кибернетики, теории информации, распознавания образов и искусственного интеллекта (М.А. Бурцев, В.Н. Вапник, А.И. Галушкин, А.В. Гасников, В.М. Глушков, А.Н. Колмогоров, С.И. Корсаков, А.А. Ляпунов, Ю.Е. Нестеров, Д.А. Поспелов, А.Я. Червоненкис и др.) в мировой научно-технический прогресс;

− готовность к обучению и заинтересованность в дальнейшей эффективной профессиональной деятельности в сфере информационных технологий, искусственного интеллекта и защиты информации для решения актуальных государственных, социальных и личностных задач.

2. Гражданское воспитание:

− осознание важности морально-этических принципов в деятельности, связанной с реализацией технологий искусственного интеллекта;

− осознание себя ответственным участником цифрового общества: понимание того, что действия в сети имеют реальные последствия для самого пользователя, его близких и окружающих, и что правовые и этические нормы распространяются на цифровую среду в полной мере;

− понимание основных преимуществ технологий искусственного интеллекта: снижение рисков, круглосуточная доступность, быстрое принятие решений, адаптируемость, снижение нагрузки на человека в рутинных

операциях, производственных процессах;

− представление о возможностях и перспективах использования искусственного интеллекта в различных областях профессиональной деятельности человека: в информационных системах связи, в транспорте и логистике доставки товаров, в финансовом секторе для фиксации и блокировки атак злоумышленников, в медицине для диагностики и поиска схем лечения пациентов, в образовании для повышения качества знаний, в бизнесе для проведения аналитики, оптимизации рутинных рабочих процессов, выявления рисков и мошенничества, в жилищно-коммунальном хозяйстве и городском управлении для систем «умного» дома и «умного» города, цифровых двойников объектов и территорий, в промышленности и сельском хозяйстве для контроля качества, в космической отрасли планирования миссий);

− готовность к активному участию в обсуждении социально значимых и этических проблем, связанных с современными технологиями, в особенности технологиями искусственного интеллекта;

− соблюдение правил безопасности в цифровой среде: устойчивые навыки безопасного поведения в интернет-среде, привычка защищать учетные записи и персональные данные, настраивать приватность сервисов и домашних устройств, не передавать конфиденциальную информацию по непроверенным каналам.

3. Духовно-нравственное воспитание:

− уважение традиционных российских духовно-нравственных ценностей;

− готовность оценивать свое поведение и поступки, а также поведение и поступки других людей с позиции нравственных и правовых норм с учетом осознания последствий поступков;

− активное неприятие асоциальных действий, в том числе в сети Интернет и в процессе взаимодействия с искусственным интеллектом (обман, мошенничество, кибербуллинг, травля, вторжение в частную жизнь других людей), а также противодействие им;

− способность критически оценивать этические и моральные аспекты использования искусственного интеллекта и выступать за ответственность (и быть ответственными) при его использовании;

− принятие базового правила безопасного использования искусственного интеллекта: совет дает ИИ, решение и ответственность остаются за человеком; непринятие позиции перекладывания ответственности за собственные решения на алгоритм или сервис;

− уважение к интеллектуальному труду и авторству, неприятие выдачи результата, созданного искусственным интеллектом или другим человеком, за собственный; следование правилам академической честности при учебной работе с ИИ-инструментами.

4. Эстетическое воспитание:

− понимание эмоционального воздействия искусства при генерировании текстов, иллюстраций, музыки с помощью искусственного интеллекта; осознание важности искусства и творчества как способов самовыражения и коммуникации;

− умение отличать творческий замысел и выбор человека от генерации ИИ по образцу; понимание того, что модель является инструментом, а автором смыслового и эстетического решения остается человек.

5. Физическое воспитание, формирование культуры здоровья и эмоционального благополучия:

− осознание возможных негативных последствий использования искусственного интеллекта с целью обеспечения физической безопасности человека, а также рисков, связанных с доверием автоматическим решениям в транспорте, медицине, системах «умного» дома и города;

− осознание необходимости обращения к родителям, педагогу или школьному психологу при переживании конфликта, травли (буллинга) и иных сложных жизненных ситуаций;

− критическое отношение к рекомендациям ИИ-сервисов в сфере здоровья и самочувствия: понимание границ их применимости, опасности самолечения и необходимости обращаться к специалисту;

− понимание влияния непрерывного пребывания в цифровой среде на самочувствие, внимание и режим и готовность дозировать цифровую активность.

6. Трудовое воспитание:

− интерес к практическому изучению профессий в сфере ИКТ, искусственного интеллекта и защиты информации, осознание их актуальности и перспективности с точки зрения выстраивания личностных жизненных траекторий, реализации общественных интересов и потребностей;

− уважение к профессиональной деятельности в сфере информационных технологий, ее результатам и достижениям;

− понимание того, что применение ИИ не снимает с человека требований качества, аккуратности и проверяемости результата работы.

7. Экологическое воспитание:

− понимание возможностей использования искусственного

интеллекта для решения экологических проблем, сохранения и улучшения окружающей среды (мониторинг состояния окружающей среды, анализ данных дистанционного зондирования Земли, рациональное использование ресурсов в системах «умного» города и сельского хозяйства);

− готовность к участию в практической деятельности экологической направленности с применением ИИ-технологий;

− осознание собственной экологической ответственности при пользовании цифровыми сервисами и устройствами: потребление электроэнергии инфраструктурой данных и электронные отходы как обратная сторона цифровизации.

8. Ценности научного познания:

− формирование представлений об информации, информационных процессах и информационных технологиях, соответствующих современному уровню развития науки и общественной практики; интерес к обучению и познанию, любознательность, стремление к самообразованию;

− понимание научного пути развития искусственного интеллекта: смена парадигм от символьных систем и экспертных систем к статистическому обучению, нейронным сетям и генеративным моделям; роль накопления данных и роста вычислительных мощностей;

− развитие навыков самостоятельной работы с информацией и средствами информационных технологий; привычка проверять полученные с помощью ИИ сведения по независимым источникам и опираться на первичные данные.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

Познавательные универсальные учебные действия

Базовые логические действия:

− выявлять и характеризовать существенные признаки объектов (явлений), в том числе понятий «данные», «алгоритм», «модель», «обучение», «признак», «угроза», «уязвимость», «защита»;

− устанавливать существенный признак классификации, основания для обобщения и сравнения, критерии проводимого анализа (например, различать задачи, которые решает обычный алгоритм, и задачи, для которых требуется обучаемая модель);

− с учетом предложенной задачи выявлять закономерности и противоречия в рассматриваемых фактах, данных и наблюдениях;

− выявлять дефициты информации, данных, необходимых для решения поставленной задачи (в том числе дефицит или смещение обучающих данных);

− выявлять причинно-следственные связи при изучении явлений и процессов, в том числе цепочку «данные - алгоритм - результат - решение человека»;

− устанавливать связи между понятиями курса информатики (измерение и представление информации, логические основы, моделирование, управление и обратная связь) и явлениями сферы искусственного интеллекта и защиты информации;

− самостоятельно выбирать способ решения учебной задачи (сравнивать несколько вариантов решения, выбирать наиболее подходящий с учетом самостоятельно выделенных критериев).

Базовые исследовательские действия:

− использовать вопросы как исследовательский инструмент познания;

− формулировать запрос к ИИ-сервису, уточнять его и изменять в зависимости от полученного результата, интерпретировать ответ и проверять его на соответствие поставленной задаче;

− формировать гипотезу об истинности собственных суждений и суждений других, аргументировать свою позицию, мнение;

− оценивать на применимость и достоверность информацию, полученную в ходе личных наблюдений, в том числе полученную с помощью инструментов искусственного интеллекта;

− самостоятельно формулировать обобщения и выводы по результатам личного наблюдения, владеть инструментами оценки достоверности полученных выводов и обобщений;

− прогнозировать возможное дальнейшее развитие процессов, событий и их последствия в аналогичных или сходных ситуациях, выдвигать предположения об их развитии в новых условиях и контекстах.

Работа с информацией:

− применять различные методы, инструменты и запросы при поиске и отборе информации или данных из источников с учетом предложенной учебной задачи и заданных критериев;

− выбирать, анализировать, систематизировать и интерпретировать информацию различных видов и форм представления (текст, изображение, звук, таблица, схема);

− находить сходные аргументы (подтверждающие или опровергающие одну и ту же идею, версию) в различных информационных источниках;

− отличать факт от оценки и мнения; оценивать надежность информации по критериям, предложенным педагогическим работником или

сформулированным самостоятельно, с учетом актуальности и первичности источника;

− распознавать признаки сфабрикованной и манипулятивной информации, в том числе созданной или измененной с помощью искусственного интеллекта, проверять изображения, ссылки и метаданные файлов;

− понимать, какие данные о пользователе собирают цифровые сервисы, осознанно работать с пользовательскими соглашениями, согласиями и настройками приватности; соблюдать правила обработки и распространения персональных данных - своих и чужих;

− эффективно запоминать и систематизировать информацию.

Коммуникативные универсальные учебные действия

Общение:

− выражать свою точку зрения в устных и письменных текстах, в том числе при взаимодействии с ИИ-сервисом (формулирование запроса и описание задачи);

− соблюдать правила сетевого этикета в переписке, комментариях и публичных выступлениях в цифровой среде;

− распознавать невербальные средства общения, понимать значение социальных знаков, знать и распознавать предпосылки конфликтных ситуаций и смягчать конфликты, вести переговоры;

− понимать намерения других, проявлять уважительное отношение к собеседнику и в корректной форме формулировать свои возражения;

− распознавать манипулятивные приемы воздействия в цифровой коммуникации (дефицит времени, страх, лесть, авторитет, жадность), отличать просьбу о конфиденциальных данных или деньгах от легитимного обращения;

− в ходе диалога и (или) дискуссии задавать вопросы по существу обсуждаемой темы и высказывать идеи, нацеленные на решение задачи и поддержание благожелательности общения;

− сопоставлять свои суждения с суждениями других участников диалога, обнаруживать различие и сходство позиций;

− своевременно и по назначению обращаться за помощью и поддержкой (к взрослым, в службу поддержки сервиса, к специалистам) при возникновении ситуации, угрожающей безопасности информации или личности.

Совместная деятельность:

− принимать цель совместной деятельности, коллективно строить

действия по ее достижению (распределять роли, договариваться, обсуждать процесс и результат совместной работы);

− уметь обобщать мнения нескольких людей, проявлять готовность руководить, выполнять поручения;

− договариваться о правилах использования ИИ-инструментов в совместной работе и открыто указывать, какая часть результата получена с их помощью.

Регулятивные универсальные учебные действия

Самоорганизация:

− выявлять проблемы для решения в жизненных и учебных ситуациях;

− самостоятельно составлять алгоритм решения задачи (или его часть), выбирать способ решения учебной задачи с учетом имеющихся ресурсов и собственных возможностей, аргументировать предлагаемые варианты решений;

− выстраивать личный регламент работы с ИИ-сервисами: с какими сервисами и для каких задач работаю, как проверяю результат, каких задач не делегирую модели, делать выбор и брать ответственность за решение.

Самоконтроль:

− владеть способами самоконтроля, самомотивации и рефлексии;

− давать адекватную оценку ситуации и предлагать план ее изменения;

− учитывать контекст и предвидеть трудности, которые могут возникнуть при решении учебной задачи, адаптировать решение к меняющимся обстоятельствам;

− соблюдать прием «пауза перед действием»: не выполнять опасное действие (переход по ссылке, перевод средств, передача кода и персональных данных) под влиянием срочности и эмоционального давления, проверять информацию по независимому каналу;

− применять правило учебной честности: сначала решить самостоятельно, потом сверяться с результатом, полученным с помощью ИИ;

− объяснять причины достижения (недостижения) результатов деятельности, давать оценку приобретенному опыту, уметь находить позитивное в произошедшей ситуации;

− вносить коррективы в деятельность на основе новых обстоятельств, изменившихся ситуаций, установленных ошибок, возникших трудностей;

− оценивать соответствие результата цели и условиям;

− фиксировать произошедший инцидент в цифровой среде (доказательства, последовательность действий) и выполнять известный алгоритм реагирования.

Эмоциональный интеллект:

− различать, называть и управлять собственными эмоциями и эмоциями других, ставить себя на место другого человека, понимать мотивы и намерения другого;

− регулировать способ выражения эмоций в цифровой коммуникации;

− сохранять самообладание в стрессовой ситуации, связанной с угрозой безопасности данных или денег, и действовать по заранее известному алгоритму.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ
5-7 классы

«Искусственный интеллект»:

− определять искусственный интеллект и приводить примеры задач, которые он решает: распознавание образов и речи, генерация текста и изображений, рекомендации, игра, планирование;

− сопоставлять человеческий интеллект и работу компьютера: называть, что ИИ делает быстрее и выносливее человека, а что по-прежнему умеет только человек;

− различать достоверную и недостоверную информацию об искусственном интеллекте, узнавать популярные мифы («восставшие машины») и отделять их от реальных возможностей технологий;

− характеризовать образ «думающей машины» в сказках, литературе, кино и мультипликации и соотносить вымысел с современными технологиями;

− называть имена отечественных ученых, чьи работы стояли у оснований кибернетики и искусственного интеллекта и приводить примеры помощи ИИ науке;

− описывать принципы работы искусственного интеллекта на уровне аналогии: мозг и нейрон, нейросеть как «сеть весов», обучение как настройка весов на примерах;

− называть сферы применения ИИ в повседневной жизни: телефон, навигатор, умная колонка, голосовой помощник, поисковые рекомендации, игры;

− объяснять на примерах применение ИИ в науке, медицине

(«второе мнение» врача), на производстве и в космосе, в «умном» доме и «умном» городе;

− раскрывать смысл понятия «цифровой двойник» и приводить примеры, где копия объекта позволяет проводить опыты без вреда для оригинала.

«Информационная безопасность»:

− называть основные правила безопасного поведения в сети и объяснять, зачем они нужны;

− объяснять, почему пароль подобен ключу от двери, составлять надежный пароль и соблюдать правило его уникальности и неразглашения;

− различать безопасные и опасные ситуации общения в сети: распознавать незнакомца, выясняющего личные сведения, и «обман на доверии» (ложная служба поддержки, розыгрыш, «срочная оплата», помощь мнимого знакомого);

− объяснять, что такое персональные данные и цифровой след, почему действия в сети запоминаются надолго и как это влияет на репутацию;

− показывать на простых примерах, кто собирает данные о пользователе (сайты и приложения), и называть базовые способы ограничить сбор – настройками приватности и разрешений;

− распознавать достоверную и недостоверную информацию, признаки выдумки и манипуляции, проверять новость по нескольким источникам;

− объяснять, как ИИ создает и изменяет изображения, звуки и видео (фейки и дипфейки), и называть простые признаки подделки;

− называть причины, по которым компьютер может «заболеть», отличать вредоносные программы и соблюдать безопасные правила загрузки и установки программ.

«Этика, право и профориентация»:

− называть простые этические правила обращения с ИИ и с информацией, полученной с его помощью;

− рассуждать о вопросе авторства сгенерированных текстов, изображений и музыки: кто автор, чей труд и чье изображение нельзя использовать без разрешения;

− называть профессии, в которых нужен искусственный интеллект, и рассказывать, что делает человек в этих профессиях;

− формулировать личное правило безопасной и честной работы с ИИ: «совет дает ИИ, решает человек».

8-9 классы

«Искусственный интеллект»:

- характеризовать основные этапы развития ИИ (символьный ИИ и экспертные системы, статистическое обучение, глубокие нейронные сети, генеративные модели и ИИ-агенты) и роль данных и вычислительных мощностей в этом развитии;
- устанавливать связь темы с курсом информатики (измерение и представление информации, логические основы, моделирование, управление и обратная связь);
- отличать рассуждение человека от ответа ИИ и формулировать уточняющие запросы;
- раскрывать границы применимости ИИ: почему модель, хорошо решающая одну задачу, беспомощна в другой; пояснять на доступном уровне смысл переобучения и смещения ошибки;
- объяснять принцип компьютерного восприятия через дискретное представление данных: пиксель и цветовая модель для зрения, частота дискретизации для звука; называть задачи и границы распознавания речи, образов и текста;
- характеризовать моделирование как метод познания и цифровой двойник как динамическую компьютерную модель объекта: экспериментировать на двойнике без риска для оригинала, роль ИИ в калибровке и прогнозе;
- рассматривать «умный» дом и «умный» город, Интернет вещей как системы управления с обратной связью: контур «датчик - сигнал - решение - исполнитель»;
- связывать работу облачных и сетевых сервисов с особенностями хранения и передачи данных и с тем, какие данные о пользователе собирают эти сервисы;
- характеризовать роль ИИ в науке, медицине, промышленности и сельском хозяйстве, космических системах; объяснять, что берет на себя ИИ и что остается ответственностью человека.

«Информационная безопасность»:

- объяснять связь между длиной пароля и числом возможных комбинаций, обосновывать требования к стойкости и уникальности пароля;
- различать факторы и способы аутентификации (пароль, одноразовый код, биометрия, аппаратный ключ), объяснять назначение двухфакторной аутентификации и менеджера паролей;
- описывать приемы социальной инженерии (дефицит времени, страх, лесть, авторитет, жадность) и типовые сценарии атак; объяснять, как

ИИ усиливает манипуляцию (подделка голоса и лица, безупречный текст, персонализация приманки);

− применять личный алгоритм противодействия информационным угрозам: пауза, проверка по независимому каналу, отказ сообщать код и персональные данные;

− распознавать фишинговые письма и ссылки, фальшивые конкурсы и «легкие деньги», поддельные службы поддержки; называть алгоритм действий при совершенном обмане (зафиксировать доказательства, сменить пароли, сообщить взрослым, обратиться в поддержку сервиса и полицию);

− выявлять признаки дипфейков и поддельного контента (артефакты, несогласованность мимики, метаданные, водяные знаки, отсутствие подтверждения в независимых источниках); применять регламент «не верь на глаз – проверь источник»;

− разграничивать факт, оценку и мнение; применять критерии достоверности и актуальности источника, перекрестную проверку и работу с первичными публикациями; объяснять, почему ответ нейросети требует такой же проверки, как любой внешний источник;

− объяснять, что такое пользовательское соглашение, политика конфиденциальности и cookie-уведомления, как их читать и находить существенные пункты, управлять разрешениями приложений и настройками приватности;

− характеризовать профилирование и персонализацию рекламы;

− классифицировать вредоносное ПО (вирусы, черви, трояны, шифровальщики, шпионское ПО), называть пути заражения и признаки;

− объяснять принцип действия антивируса и роль машинного обучения в обнаружении новых образцов, обосновывать важность обновлений и резервного копирования;

− называть типовые уязвимости устройств Интернета вещей (пароли по умолчанию, уязвимые прошивки, открытые сети) и меры защиты домашней сети;

− соблюдать правовые основы работы с персональными данными: категории данных, согласие на обработку, права субъекта и обязанности оператора; объяснять особую чувствительность биометрических и медицинских данных;

− оценивать риски слежки и потери контроля при массовом сборе данных, называть этические и правовые ограничения работы с биометрией.

«Этика, право, регулирование и профориентация»:

− называть этические принципы ИИ (справедливость, прозрачность, объяснимость, безопасность, подотчетность);

− характеризовать российское регулирование ИИ (национальный проект «Искусственный интеллект»), понимать права человека в среде ИИ-сервисов, защиту от дискриминации алгоритмами, право на объяснение, принцип «человек принимает решение»;

− называть профессии цикла данных и ИИ и профессии информационной безопасности, описывать их задачи и востребованные школьные знания;

− соотносить индивидуальную образовательную траекторию с требованиями ОГЭ и профильными предметами; планировать дальнейший выбор с опорой на изученные области ИИ и ИБ;

− сформулировать и применять личный регламент работы с ИИ-сервисами и базовые правила информационной безопасности; закреплять ключевое правило курса: совет дает ИИ, решает человек.