Государственное бюджетное общеобразовательное учреждение Самарской области основная общеобразовательная школа № 9 имени Героя Советского Союза И.Д. Ваничкина города Новокуйбышевска городского округа Новокуйбышевск Самарской области 446218, Самарская область, г. Новокуйбышевск, ул. Ворошилова, д. 6, тел. 4-70-52

РАССМОТРЕНО	ПРОВЕРЕНО	УТВЕРЖДЕНО
на заседании	Зам. директора по УВР	Директор ГБОУ ООШ № 9
Методического совета	_____ М.В. Корнилина	г. Новокуйбышевска
протокол № 2	от 02.11.2026 г.	Приказ № 346-од
от 02.11.2026 г.		от 03.11.2026 г.
		_____ Г.Н. Недбало

Рабочая программа
внеурочной деятельности
«Искусственный интеллект
и информационная безопасность»
(7–9 классы)

Составитель:
Хабибулин Раис Маратович,
учитель информатики

ЭП

Недбало Г_Н_
C=RU, O=ГБОУ ООШ № 9, CN=Недбало Г_Н_, E=pu_sch9_nkb@63edu.ru
00afd8c98ff6d05c5c
2026-11-03 14:10:02

ВВЕДЕНИЕ

Рабочая программа внеурочной деятельности учебного курса «Искусственный интеллект и информационная безопасность» (далее — Программа) предназначена для обучающихся 7–9 классов. Программа рассчитана на 1 час в неделю, 27 занятий.

Программа включает три раздела:

- планируемые результаты освоения курса внеурочной деятельности;
- содержание курса внеурочной деятельности;
- тематическое планирование.

Программа разработана в соответствии:

• с федеральным государственным образовательным стандартом основного общего образования, утверждённым приказом Минпросвещения России от 31.05.2021 № 287 и от 18.06.2025 № 467;

• с федеральной образовательной программой основного общего образования, утверждённой приказом Минпросвещения России от 18.05.2023 № 370;

• с основной образовательной программой основного общего образования ГБОУ ООШ № 9 г. Новокуйбышевска;

• с учётом положений Стратегии научно-технологического развития Российской Федерации, Национальной стратегии развития искусственного интеллекта на период до 2030 года и федерального проекта «Искусственный интеллект».

Содержание программы выстроено вокруг сквозной идеи: на уровне 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.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Личностные результаты:

• понимание роли науки и технологий, в том числе информационных и коммуникационных, в обеспечении устойчивого развития российского государства и общества;

• ценностное отношение к достижениям российских учёных, инженеров и специалистов в области информатики, кибернетики, искусственного интеллекта и защиты информации;

• осознание себя ответственным участником цифрового общества: понимание того, что действия в сети имеют реальные последствия для самого пользователя, его близких и окружающих;

• сформированность понимания ценности безопасного образа жизни, правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде;

• принятие базового правила безопасного использования искусственного интеллекта: совет даёт ИИ, решение и ответственность остаются за человеком;

• готовность критически оценивать этические и моральные аспекты использования искусственного интеллекта и нести ответственность за собственные решения.

Метапредметные результаты:

Регулятивные универсальные учебные действия:

• выявлять проблемы для решения в жизненных и учебных ситуациях, самостоятельно составлять алгоритм решения задачи;

• выстраивать личный регламент работы с ИИ-сервисами: с какими сервисами и для каких задач работать, как проверять результат, какие задачи не делегировать модели;

• соблюдать приём «пауза перед действием»: не выполнять опасное действие 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;

• оценивать соответствие результата цели и условиям, вносить коррективы в деятельность на основе новых обстоятельств.

Познавательные универсальные учебные действия:

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

• устанавливать связи между понятиями курса информатики и явлениями сферы искусственного интеллекта и защиты информации;

• формулировать запрос к ИИ-сервису, уточнять его и изменять в зависимости от полученного результата, интерпретировать ответ и проверять его;

• применять различные методы, инструменты и запросы при поиске и отборе информации, анализировать, систематизировать и интерпретировать информацию различных видов;

• отличать факт от оценки и мнения; оценивать надёжность информации по предложенным критериям;

• распознавать недостоверную и манипулятивную информацию, проверять новость по нескольким источникам.

Коммуникативные универсальные учебные действия:

• строить позитивные отношения в процессе учебной и познавательной деятельности;

• критически относиться к собственному мнению, признавать ошибочность своего мнения и корректировать его;

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

• целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;

• использовать информацию с учётом этических и правовых норм;

• создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Предметные результаты:

• характеризовать основные этапы развития искусственного интеллекта, роль данных и вычислительных мощностей;

• отличать рассуждение человека от ответа ИИ и формулировать уточняющие запросы;

• раскрывать границы применимости ИИ: почему модель, хорошо решающая одну задачу, беспомощна в другой;

• объяснять принцип компьютерного восприятия через дискретное представление данных: пиксель и цветовая модель для зрения, частота дискретизации для звука;

• характеризовать моделирование как метод познания и цифровой двойник как динамическую компьютерную модель объекта;

• объяснять связь между длиной пароля и числом возможных комбинаций, обосновывать требования к стойкости и уникальности пароля;

• различать факторы и способы аутентификации, объяснять назначение двухфакторной аутентификации и менеджера паролей;

• описывать приёмы социальной инженерии и типовые сценарии атак, объяснять, как ИИ усиливает манипуляцию;

• распознавать фишинговые письма и ссылки, фальшивые конкурсы, поддельные службы поддержки;

• выявлять признаки дипфейков и поддельного контента, применять регламент «не верь глазам — проверь источник»;

• разграничивать факт, оценку и мнение, применять критерии достоверности и актуальности источника;

• объяснять, что такое пользовательское соглашение, политика конфиденциальности и cookie-уведомления;

• классифицировать вредоносное ПО, называть пути заражения и признаки, объяснять принцип действия антивируса;

• называть типовые уязвимости устройств Интернета вещей и меры защиты домашней сети;

• соблюдать правовые основы работы с персональными данными, объяснять особую чувствительность биометрических и медицинских данных;

• называть этические принципы ИИ: справедливость, прозрачность, объяснимость, безопасность, подотчётность;

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

• формулировать и применять личный регламент работы с ИИ-сервисами и базовые правила информационной безопасности.

СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Содержание программы интегрирует знания различных учебных предметов, направлено на формирование межпредметных связей с информатикой, развитие компетенций обучающихся в области современных информационных и коммуникационных технологий, 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, умений эффективно их использовать, свободно ориентироваться в цифровой среде и ответственно вести себя в ней с точки зрения информационной безопасности.

Основными **целями** изучения учебного курса являются:

• получение обучающимися знаний, умений и навыков в области искусственного интеллекта и информационной безопасности;

• формирование критического отношения к информации и коммуникации в цифровом пространстве в условиях обеспечения информационной безопасности;

• воспитание ответственного отношения к воспринимаемой информации с учётом этических норм её использования и распространения;

• формирование стремления к продолжению образования в области искусственного интеллекта и продуктивной деятельности с применением технологий ИИ.

Задачи программы:

• овладение знаниями об основах искусственного интеллекта и его применении в современном мире, технологиях ИИ, вызовах и ограничениях ИИ, 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 ИИ;

• формирование умений обоснованно и ограниченно использовать разрешённые педагогом инструменты ИИ для отдельных учебных действий с обязательной проверкой результата;

• формирование умений пользоваться сервисами для синтеза речи, генерировать тексты и изображения с помощью ИИ, 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 её 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, основ работы с данными, коммуникации на современных цифровых платформах, информационной безопасности.

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.

7 КЛАССЫ (27 Ч.)

Занятие 1. Искусственный интеллект и как с ним общаться безопасно. 1 час.

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 даёт ИИ, а решает человек. ИИ не может заменить родителей, друзей или психолога. Риск доверительных отношений с ИИ.

Занятие 2. Эволюция нейросетей и информационная безопасность. 1 час.

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 её боятся потерять. Информацию можно создать, передать, потерять или украсть. Какую информацию нельзя доверять нейросети.

Занятие 3. Вклад российских учёных в развитие искусственного интеллекта. 1 час.

Как ИИ помогает учёным делать открытия: быстрый перебор вариантов, поиск закономерностей в больших данных, предсказывание свойств веществ. Российские учёные, исследования которых стали основанием для возникновения ИИ: 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. 1 час.

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. 1 час.

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. Насколько 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. 1 час.

Как писатели, режиссёры 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 влечёт угрозы, которые нужно уметь узнавать.

Занятие 7. Этика и мораль для искусственного интеллекта. 1 час.

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. 1 час.

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. 1 час.

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 надёжным. 1 час.

Пароль как ключ от «цифровой комнаты». Зачем нужны пароли и почему их нельзя никому сообщать, даже друзьям. Признаки надёжного 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. 1 час.

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». 1 час.

У компьютера свои «органы чувств» (датчики и сенсоры): программа распознаёт 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: всё сохраняется надолго. 1 час.

Что такое персональные данные: адрес, телефон, школа, фото в социальных сетях. Почему всё, 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. Правила обращения с данными при выполнении учебных заданий.

Занятие 14. Кто собирает мои данные: настройки и согласия сайтов. 1 час.

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. 1 час.

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 всё измеряет и собирает данные о людях, стирается граница приватности.

Занятие 16. Цифровые двойники: точная копия для опытов без вреда. 1 час.

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 самолёта или завода: как инженеры тестируют новые детали в виртуальном мире.

Занятие 17. Подделка и обман: как ИИ создаёт фейки и как их узнать. 1 час.

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. 1 час.

Приманка всегда выглядит заманчиво или страшно, её цель — вывести из безопасного интернет-пространства. Подозрительные письма и ссылки (письма-приманки), фальшивые подарки, конкурсы и «лёгкие 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 ещё убедительнее. Что делать, если обман уже произошёл? 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. 1 час.

Нейросеть — это советчик и тренажёр, 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 своё; обязательно проверяй ответы ИИ на ошибки.

Занятие 20. ИИ рисует и сочиняет: кто здесь автор. 1 час.

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. 1 час.

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. 1 час.

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. 1 час.

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. 1 час.

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 берёт ИИ, часть остаётся 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. 1 час.

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

Занятие 26. Кем быть: профессии, где нужен искусственный интеллект. 1 час.

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. 1 час.

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

8 КЛАСС (27 Ч.)

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

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 задаётся жёсткой инструкцией. Границы применимости: почему модель ИИ, хорошо решающая одну задачу, беспомощна в другой. Ключевое правило: совет даёт ИИ, а решение и ответственность — за человеком.

Занятие 2. Эволюция идей искусственного интеллекта: от логических правил к обучению на данных. 1 час.

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 учёных в развитие искусственного интеллекта. 1 час.

Как ИИ помогает науке делать открытия: быстрый перебор вариантов, поиск закономерностей в больших данных, предсказание свойств веществ, обработка результатов наблюдений. Учёные, чьи работы стали основанием для возникновения ИИ и способствовали его развитию: 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. 1 час.

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 её проверки: факт, оценка, источник. 1 час.

Разграничение факта, оценки и мнения. Критерии достоверности и актуальности. Перекрёстная 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. 1 час.

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 приём. Реальные риски связаны со злоупотреблением технологиями: слежкой, дезинформацией, манипуляцией и утратой контроля. Умение узнавать настоящие угрозы.

Занятие 7. Этика и правовое регулирование искусственного интеллекта. 1 час.

Этические принципы ИИ: справедливость, прозрачность, объяснимость, безопасность, подотчётность. 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. 1 час.

Психологические приёмы: 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. 1 час.

Как устроены привычные сервисы: поисковая выдача и рекомендации, переводчики, распознавание речи, автодополнение, навигация, голосовые помощники. Понятие обучаемой модели и её 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. 1 час.

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. 1 час.

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. 1 час.

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. 1 час.

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. Правила обращения с данными при выполнении учебных заданий.

Занятие 14. Согласия, настройки приватности и профилирование: кто и как собирает данные. 1 час.

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. 1 час.

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. 1 час.

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. 1 час.

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. 1 час.

Типовые схемы: фишинговые письма и ссылки, фальшивые конкурсы и «лёгкие 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 произошёл: 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. 1 час.

Роль ИИ в учебной работе: разобрать сложное, составить вопросы для самопроверки, проверить черновик, стать тренажёром формулировок. Приёмы 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 своё. «Ручная» проверка результатов работы ИИ: существование приведённых ссылок, документов, цитат и статистических данных.

Занятие 20. Генеративный ИИ и авторское право: кто автор созданного ИИ произведения. 1 час.

Как реализуется генерация текста, изображений и музыки: ИИ — инструмент, а самостоятельный творческий этап, предшествующий обращению к сервису ИИ, остаётся 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 ответственно относиться к труду.

Занятие 21. ИИ на службе медицины: задачи диагностики, ограничения, ответственность. 1 час.

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. 1 час.

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. 1 час.

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. 1 час.

Задачи ИИ на производстве: компьютерное зрение для контроля качества, роботизированные линии, умное сельское хозяйство и транспорт. Что остаётся человеку: часть работы берёт 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. 1 час.

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 её последствия для управления. Угрозы передачи данных между Землёй и космосом: перехват сигнала, подмена команд и телеметрии, компрометация наземного сегмента.

Занятие 26. Профессии на стыке ИИ и информационной безопасности: требования и траектории. 1 час.

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. 1 час.

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

9 КЛАСС (27 Ч.)

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

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 задаётся жёсткой инструкцией. Границы применимости: почему модель ИИ, хорошо решающая одну задачу, беспомощна в другой. Ключевое правило: совет даёт ИИ, а решение и ответственность — за человеком.

Занятие 2. Эволюция идей искусственного интеллекта: от логических правил к обучению на данных. 1 час.

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 учёных в развитие искусственного интеллекта. 1 час.

Как ИИ помогает науке делать открытия: быстрый перебор вариантов, поиск закономерностей в больших данных, предсказание свойств веществ, обработка результатов наблюдений. Учёные, чьи работы стали основанием для возникновения ИИ и способствовали его развитию: 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. 1 час.

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 её проверки: факт, оценка, источник. 1 час.

Разграничение факта, оценки и мнения. Критерии достоверности и актуальности. Перекрёстная 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. 1 час.

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 приём. Реальные риски связаны со злоупотреблением технологиями: слежкой, дезинформацией, манипуляцией и утратой контроля. Умение узнавать настоящие угрозы.

Занятие 7. Этика и правовое регулирование искусственного интеллекта. 1 час.

Этические принципы ИИ: справедливость, прозрачность, объяснимость, безопасность, подотчётность. 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. 1 час.

Психологические приёмы: 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. 1 час.

Как устроены привычные сервисы: поисковая выдача и рекомендации, переводчики, распознавание речи, автодополнение, навигация, голосовые помощники. Понятие обучаемой модели и её 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. 1 час.

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. 1 час.

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. 1 час.

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. 1 час.

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. Правила обращения с данными при выполнении учебных заданий.

Занятие 14. Согласия, настройки приватности и профилирование: кто и как собирает данные. 1 час.

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. 1 час.

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. 1 час.

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. 1 час.

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. 1 час.

Типовые схемы: фишинговые письма и ссылки, фальшивые конкурсы и «лёгкие 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 произошёл: 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. 1 час.

Роль ИИ в учебной работе: разобрать сложное, составить вопросы для самопроверки, проверить черновик, стать тренажёром формулировок. Приёмы 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 своё. «Ручная» проверка результатов работы ИИ: существование приведённых ссылок, документов, цитат и статистических данных.

Занятие 20. Генеративный ИИ и авторское право: кто автор созданного ИИ произведения. 1 час.

Как реализуется генерация текста, изображений и музыки: ИИ — инструмент, а самостоятельный творческий этап, предшествующий обращению к сервису ИИ, остаётся 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 ответственно относиться к труду.

Занятие 21. ИИ на службе медицины: задачи диагностики, ограничения, ответственность. 1 час.

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. 1 час.

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. 1 час.

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. 1 час.

Задачи ИИ на производстве: компьютерное зрение для контроля качества, роботизированные линии, умное сельское хозяйство и транспорт. Что остаётся человеку: часть работы берёт 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. 1 час.

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 её последствия для управления. Угрозы передачи данных между Землёй и космосом: перехват сигнала, подмена команд и телеметрии, компрометация наземного сегмента.

Занятие 26. Профессии на стыке ИИ и информационной безопасности: требования и траектории. 1 час.

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. 1 час.

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

Формы организации:

- традиционное занятие (коллективная и групповая формы работы);
- тренинги (в классической форме и по кейс-методу);
- дистанционное обучение (видеоролики, почтовые рассылки);
- диспуты;
- игры, викторины, квесты, разбор кейсов, тренажёры;
- проекты;
- общественно-полезные практики.

Виды деятельности:

- познавательная;
- проблемно-ценностное общение;
- техническое творчество;
- проектная деятельность.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

Согласно плану внеурочной деятельности ГБОУ ООШ № 9 г. Новокуйбышевска на реализацию рабочей программы учебного курса «Искусственный интеллект и информационная безопасность» выделено по 1 часу в неделю. Программа реализуется в 7–9 классах — 27 ч. При необходимости образовательная организация может использовать резерв учебного времени на повторение, проектную деятельность и волонтёрскую практику.

7 КЛАССЫ (27 Ч.)

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
1	Искусственный интеллект и как с ним общаться безопасно	1	ИИ решает задачи, которые раньше умел решать только человек. Мифы и реальность. Главное правило: совет даёт ИИ, решает человек. Риск доверительных отношений с ИИ.	Рассказывает, что такое ИИ и какие задачи он решает. Отличает мифы от реальных возможностей технологий. Формулирует правило «совет даёт ИИ, а решает человек».
2	Эволюция нейросетей и информационная безопасность	1	От первых программ и шахмат до голосовых помощников и ИИ-агентов. Приоритет отечественных технологий ИИ. Риски применения ИИ. Информацию можно создать, передать, потерять или украсть.	Характеризует основные этапы развития ИИ. Объясняет, почему с ростом «умности» компьютера важны навыки безопасного обращения с данными.
3	Вклад российских учёных в развитие искусственного интеллекта	1	Как ИИ помогает учёным делать открытия. Российские учёные: 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.	Характеризует вклад отечественных учёных. Приводит примеры использования ИИ в научных исследованиях.
4	Как мы думаем и как «думает» компьютер: про нейроны и нейросети	1	Головной мозг и нейроны. Почему современная нейросеть подсказана устройством мозга, но «думает» по-другому. Как распознать, рассуждает ли человек или ИИ вместо него.	Находит сходство и отличия мышления человека и работы компьютера. Объясняет принцип работы нейросети на уровне аналогии.
5	Правда или выдумка: учимся проверять информацию	1	Отличие факта от мнения. Признаки ложной публикации. Проверка источника. ИИ тоже генерирует недостоверные факты. Культурное и мировоззренческое содержание ответов ИИ.	Различает факт и мнение. Проверяет информацию по нескольким источникам. Оценивает ответы ИИ как источник, требующий проверки.

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
6	Фантастика в прошлом — реальность в настоящем	1	Образ умных машин в литературе, кино и живописи. Что стало технологией. Почему «злой робот из кино» — не настоящая опасность. Реальные риски использования ИИ.	Соотносит образ «думающей машины» с современными технологиями. Различает достоверную и недостоверную информацию об ИИ.
7	Этика и мораль для искусственного интеллекта	1	Правила, которым компьютер учат люди. Право и защита человека от злоупотреблений ИИ. Главное правило — «решает человек». Нравственная оценка поступка осуществляется человеком.	Раскрывает смысл этики и морали ИИ. Приводит примеры применения правила «решает человек». Оценивает этические ситуации.
8	Обманывать в сети тоже плохо. Обман на доверии	1	Признаки манипуляции в переписке и по телефону. Признаки вербовки детей. Алгоритм действий: не выполнять поручения незнакомцев, сообщить взрослым, сохранить переписку. Подделка голоса и лица с помощью ИИ.	Характеризует приёмы обмана. Выявляет признаки манипуляции. Объясняет, как ИИ делает обман убедительнее.
9	ИИ вокруг нас каждый день: телефон, навигатор, умная колонка	1	Переводчик, проверка орфографии, рекомендации, навигатор, голосовой помощник, распознавание фото. Помощники собирают данные о нас. Как себя защитить.	Приводит примеры ИИ-помощников. Объясняет, какие данные собирают помощники. Называет способы защиты.
10	Пароль как ключ от двери: делаем его надёжным	1	Признаки надёжного пароля. Опасность одного пароля на все сайты. Менеджер паролей и двухфакторная проверка. Как ИИ угадывает простые пароли. Проверка разрешений приложений. «Угон» аккаунтов через код из СМС.	Составляет надёжные пароли. Соблюдает правило уникальности и неразглашения. Объясняет назначение менеджера паролей и двухфакторной проверки.
11	Общаемся в сети безопасно: мессенджеры и незнакомцы	1	Сетевой этикет. Действия при травле. Опасные знакомства. Просьба включить геолокацию или уйти в личный чат — повод насторожиться. Защита смартфона.	Применяет правила безопасного общения. Распознаёт опасные знакомства. Формулирует правила поведения в группе.
12	Как ИИ «видит», «слышит», «говорит»	1	Датчики и сенсоры. Распознавание лица и текста на фото, преобразование голоса в текст и обратно. Трудности распознавания шутки и двусмысленности. Риски слежки.	Сравнивает зрение, слух и речь человека и компьютера. Объясняет трудности распознавания. Называет риски слежки.

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
13	Мои данные и цифровой след: всё сохраняется надолго	1	Персональные данные. Цифровой след. Цифровая репутация и ответственная публикация. ИИ обучается на данных и распознаёт людей. Правила обращения с данными при учебных заданиях.	Раскрывает понятия «персональные данные» и «цифровой след». Объясняет, почему данные сохраняются надолго. Анализирует собственные цифровые следы.
14	Кто собирает мои данные: настройки и согласия сайтов	1	Как сайты и приложения собирают данные. Настройки приватности и геолокация. Почему просят «подтвердить возраст картой». Как данные питают ИИ-рекомендации. Поиск жертв для мошенничества.	Настраивает приватность и разрешения. Читает простые правила согласия. Объясняет, как данные влияют на показываемый контент.
15	«Умный» дом и «умный» город: как техника заботится о нас	1	Умные устройства собирают данные с датчиков и принимают решения. ИИ в транспорте и городской среде. Стирание границы приватности при массовом сборе данных.	Описывает контур «датчик — решение — исполнитель». Объясняет, как в «умном» городе стирается граница приватности.
16	Цифровые двойники: точная копия для опытов без вреда	1	Виртуальная копия реального объекта. Опыты без вреда для оригинала. Чувствительность данных двойника. Использование копии против оригинала.	Раскрывает смысл понятия «цифровой двойник». Называет плюсы и минусы цифровой копии. Приводит примеры.
17	Подделка и обман: как ИИ создаёт фейки и как их узнать	1	Синтетические подделки: видео, голос, сообщения. Признаки подделки. ИИ помогает мошенникам и защитникам. Не сообщать код из СМС даже «другу».	Объясняет, как ИИ создаёт подделки. Выявляет признаки подделки. Применяет регламент проверки источника.
18	Ловушки в сети: как распознать мошенника	1	Письма-приманки, фальшивые подарки, конкурсы, «лёгкие деньги». Переход из игрового чата в мессенджер. Просьба сфотографировать экран телефона родителя. Таймер обратного отсчёта. Действия после обмана.	Выявляет признаки приманки. Объясняет, как ИИ делает приманки убедительнее. Характеризует алгоритм действий после обмана.
19	Учусь честно: нейросеть мне помогает, а не делает работу за меня	1	Нейросеть как советчик и тренажёр. Запрос разбора непонятного и вопросов для самопроверки. Правила честности. Проверка ответов ИИ на ошибки.	Демонстрирует последовательность: самостоятельная попытка, обращение к подсказке, проверка, объяснение решения. Соблюдает правила честности.
20	ИИ рисует и сочиняет: кто здесь автор	1	Генерация текста, изображений и мелодий по заданию	Различает творчество человека и ИИ. Раскрывает вопрос

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
			человека. Замысел и выбор остаются за человеком. Отметка ИИ-контента. Авторские права. Честное использование.	авторства. Отмечает работу, выполненную с помощью ИИ.
21	ИИ на страже здоровья: границы доверия	1	Что замечает человек и что выявляет ИИ. Анализ показателей гаджетов, снимков и кардиограмм. Самолечение по совету ИИ опасно. Безопасность медицинских данных.	Характеризует возможности ИИ в диагностике. Объясняет, почему диагноз и забота о пациенте остаются ответственностью врача.
22	Безопасность финансовых средств в цифровой среде	1	Онлайн-банкинг и приложения. Защита платежей и данных. Голосовая биометрия. Типовые схемы атак на семейный бюджет.	Объясняет, как банк защищает платежи. Приводит примеры схем обмана. Соблюдает правило: не сообщать коды и данные карты.
23	Почему «заболел» компьютер: вредоносные программы	1	Вирусы и опасные файлы. Непроверенные источники. Безопасная загрузка программ. Роль антивируса. ИИ помогает антивирусам и мошенникам.	Раскрывает смысл понятия «вредоносные программы». Называет признаки заражения. Соблюдает правила безопасной загрузки.
24	ИИ на заводе и в поле: быстрее, больше, лучше	1	Робот-сборщик, проверка деталей, умное сельское хозяйство и транспорт. Часть работы берёт ИИ, ответственность остаётся за человеком. Уязвимость «умного» производства к атакам.	Характеризует возможности ИИ в промышленности и сельском хозяйстве. Объясняет, почему «умное» производство нужно защищать.
25	Искусственный интеллект и информационная безопасность в космосе	1	Распознавание снимков Земли, планирование миссий, поиск сигналов. Космические системы связи. Угрозы передачи данных между Землёй и космосом.	Приводит примеры применения ИИ в космосе. Характеризует риски при передаче данных. Называет угрозы каналов связи.
26	Кем быть: профессии, где нужен искусственный интеллект	1	Профессии, связанные с ИИ и данными. Кто обучает, проверяет и защищает ИИ. Навыки, которые пригодятся. Специалист по кибербезопасности.	Перечисляет профессии в сфере ИИ и ИБ. Описывает их функции. Соотносит задачи профессии со школьными знаниями.
27	Я, нейросеть и моя безопасность: итоговый разговор	1	Личный «паспорт безопасности». Итоги: «ИИ — это…», «он умеет…», «в нём нельзя…», «как я себя берегу». Правило: совет даёт ИИ, решает человек.	Повторяет изученный материал. Собирает личный «паспорт безопасности». Формулирует обобщающие суждения.
Итого		**27**		

8 КЛАССЫ (27 Ч.)

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
1	Искусственный интеллект: какие задачи он решает и где ошибается	1	Задачи, которые ИИ решает на уровне человека. Отличие обучаемой модели от обычной программы. Границы применимости. Ключевое правило: совет даёт ИИ, решение и ответственность — за человеком.	Объясняет отличие обучаемой модели от обычной программы. Характеризует границы применимости. Формулирует ключевое правило.
2	Эволюция идей искусственного интеллекта: от логических правил к обучению на данных	1	Символический ИИ, экспертные системы, статистическое обучение, генеративные алгоритмы, ИИ-агенты. Роль данных и вычислительных мощностей. Контроль человека. Отечественная микроэлектроника и центры обработки данных.	Описывает основные этапы развития ИИ. Анализирует роль данных и мощностей. Характеризует новые риски и необходимость контроля человека.
3	Вклад отечественных учёных в развитие искусственного интеллекта	1	Помощь ИИ науке. Учёные: 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.	Характеризует вклад отечественных учёных. Приводит примеры использования ИИ в науке. Работает с ресурсами сети для сбора сведений.
4	Как устроена искусственная нейронная сеть: от формального нейрона к обучаемой модели	1	Мозг и нейрон как источник аналогии. Математическая модель нейрона. Статистический характер вывода. Как отличить рассуждение человека от ответа ИИ. Уточняющие запросы.	Характеризует статистический характер вывода. Формулирует уточняющие запросы. Отличает рассуждение человека от ответа ИИ.
5	Достоверность информации и методы её проверки: факт, оценка, источник	1	Факт, оценка и мнение. Критерии достоверности и актуальности. Перекрёстная проверка. Культурное и мировоззренческое содержание ответов ИИ. Признаки сфабрикованной информации. Проверка изображений, ссылок и метаданных. «Галлюцинации» ИИ.	Разграничивает факт, оценку и мнение. Применяет критерии достоверности. Проверяет метаданные и водяные знаки. Оценивает ответ нейросети как источник.
6	От научной фантастики к инженерии: какими представляли умные машины и что стало технологией	1	Образ «думающей машины» в литературе, кино и искусстве. Что сбылось, что осталось метафорой. «Восставший робот» — сюжетный приём.	Соотносит образ «думающей машины» с современными технологиями. Объясняет разницу между сюжетным приёмом и реальными рисками.

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
			Реальные риски: слежка, дезинформация, манипуляция, утрата контроля.	Характеризует реальные угрозы.
7	Этика и правовое регулирование искусственного интеллекта	1	Этические принципы ИИ: справедливость, прозрачность, объяснимость, безопасность, подотчётность. Права человека в среде ИИ-сервисов. Защита от дискриминации алгоритмами. Право на объяснение. Принцип «человек принимает решение».	Называет этические принципы ИИ. Характеризует права человека в среде ИИ-сервисов. Обосновывает принцип «человек принимает решение».
8	Социальная инженерия: как обманывают не компьютер, а человека	1	Психологические приёмы: дефицит времени, страх, лесть, авторитет, жадность. Типовые сценарии. Вербовка подростков. «Несложные поручения» как вовлечение в уголовно наказуемую деятельность. Как ИИ усиливает манипуляцию. Личный алгоритм защиты.	Описывает психологические приёмы обмана. Характеризует типовые сценарии. Применяет личный алгоритм: пауза, проверка по независимому каналу, отказ называть код и персональные данные.
9	ИИ в повседневных цифровых сервисах: принципы работы, настройки, приватность	1	Поисковая выдача, рекомендации, переводчики, распознавание речи, автодополнение, навигация, голосовые помощники. Обучаемая модель и её зависимость от данных пользователя. Настройки приватности и разрешения приложений.	Анализирует принципы работы привычных сервисов. Объясняет зависимость модели от данных пользователя. Ограничивает сбор данных настройками.
10	Аутентификация и защита доступа	1	Пароль как ключ доступа. Длина пароля, алфавит и число комбинаций. Менеджеры паролей, двухфакторная аутентификация, одноразовые коды. Биометрия и аппаратные ключи. Уникальность пароля. Проверка утечек, аудит cookie и трекеров. «Угон» через код из СМС. Как ИИ помогает атакующим.	Объясняет связь длины пароля и числа комбинаций. Различает факторы аутентификации. Обосновывает требования к стойкости и уникальности пароля. Настраивает двухфакторную защиту.
11	Безопасное общение в цифровой среде: сетевой этикет, анонимность, верификация собеседника	1	Сетевой этикет. Кибербуллинг и противодействие. Правовые последствия травли и распространения личной информации. Горячие линии. Принцип «по другую сторону экрана может быть человек и ИИ-агент». Верификация собеседника. Признаки	Понимает, что по переписке нельзя надёжно установить личность. Применяет правила проверки. Характеризует способы противодействия кибербуллингу. Верифицирует собеседника.

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
			опасных знакомств. Защита устройства и аккаунтов.	
12	Компьютерное распознавание изображений, речи и текста: признаки, модели, ошибки	1	Дискретное представление изображений и звука. Распознавание речи и синтез голоса. Оптическое распознавание текста. Компьютерное зрение. Генерация изображений по описанию. Трудности распознавания. Риск слежки и этические ограничения биометрии.	Объясняет принцип компьютерного восприятия через дискретное представление данных. Характеризует задачи распознавания и типичные ошибки. Оценивает риски слежки.
13	Персональные данные, цифровой след и цифровая репутация	1	Персональные данные и их защита. Права субъекта данных. Цифровой след: cookie, метаданные, публикации, геолокация. Как ИИ связывает данные в профиль. Управление цифровой репутацией. Правила обращения с данными при учебных заданиях.	Раскрывает, что относится к персональным данным. Характеризует цифровой след. Объясняет, как ИИ связывает данные в профиль. Управляет цифровой репутацией.
14	Согласия, настройки приватности и профилирование: кто и как собирает данные	1	Пользовательские соглашения, политики конфиденциальности, cookie-уведомления. Разрешения приложений. Профилирование и персонализация рекламы. Как данные питают ИИ-рекомендации. Как ИИ-системы ищут жертв мошенничества.	Читает соглашения и политики конфиденциальности. Настраивает разрешения приложений. Характеризует профилирование и персонализацию рекламы.
15	Промышленный и бытовой интернет вещей в умном городе: автоматизация, обратная связь, большие данные	1	Бытовой и промышленный Интернет вещей. Сбор данных с датчиков и принятие решений. Безопасность Интернета вещей: пароли по умолчанию, уязвимые прошивки, открытые сети. Защита домашней сети. Большие данные и граница приватности.	Описывает контур «датчик — сигнал — решение — исполнитель». Анализирует пользу больших данных и границу приватности. Характеризует типовые уязвимости IoT.
16	Цифровые двойники	1	Цифровой двойник как компьютерная модель объекта. Роль ИИ в калибровке и прогнозировании. Риски: чувствительность данных двойника, возможность использовать копию против оригинала.	Раскрывает смысл понятия «цифровой двойник». Характеризует роль ИИ в калибровке и прогнозировании. Оценивает риски использования копии против оригинала.

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
17	Синтетические медиа: дипфейки и методы их обнаружения	1	Генерация реалистичных видео, аудио и изображений. Признаки подделки: артефакты, несогласованность мимики, метаданные, водяные знаки, отсутствие подтверждения. ИИ на стороне подделки и защиты. Регламент проверки.	Объясняет принцип генерации реалистичных медиа. Выявляет признаки подделки. Применяет регламент «не верь глазам — проверь источник, уточни у адресата, не сообщай коды».
18	Онлайн-мошенничество: технические и социальные механизмы, действия после инцидента	1	Фишинговые письма и ссылки, фальшивые конкурсы, поддельные службы поддержки, мошенничество с картами. ИИ усиливает приманки. Алгоритм действий после обмана. Подача заявления через электронную приёмную МВД. Доказательства. Последствия участия подростков в мошенничестве.	Классифицирует типовые схемы. Объясняет, как ИИ усиливает приманки. Характеризует алгоритм действий после инцидента: зафиксировать доказательства, сменить пароли, сообщить взрослым, обратиться в поддержку и полицию.
19	Нейросеть как инструмент обучения, а не замена мышлению: академическая честность	1	Роль ИИ в учебной работе. Приёмы формулирования запроса. Обязательная проверка результата. Распознавание ошибок модели. Ссылка на источник и авторство идеи. Правила честности. «Ручная» проверка ссылок, документов, цитат и статистических данных.	Демонстрирует последовательность: самостоятельная попытка, фиксация затруднения, ограниченная подсказка, проверка, объяснение решения. Соблюдает академическую честность.
20	Генеративный ИИ и авторское право: кто автор созданного ИИ произведения	1	Генерация текста, изображений и музыки. ИИ — инструмент, творческий этап остаётся за человеком. Правовой статус сгенерированного контента. Авторское право, права на изображение и голос. Договоры с сервисами. Маркировка ИИ-контента. Этика использования.	Объясняет принцип генерации. Различает правовой статус сгенерированного контента. Отмечает работу, выполненную с помощью ИИ. Ответственно относится к чужому труду.
21	ИИ на службе медицины: задачи диагностики, ограничения, ответственность	1	Распознавание медицинских изображений и сигналов. ИИ как «второй взгляд», но не замена врача. Ответственность врача. Опасность самолечения. Фитнес-устройства и рекомендации. Безопасность передачи медицинских данных и настройка доступа.	Характеризует задачи компьютерного распознавания медицинских изображений. Объясняет, почему ИИ не заменяет врача. Оценивает качество модели через цену ошибок. Называет медицинские данные особо чувствительными.
22	Безопасность финансовых средств в	1	Онлайн-банкинг и мобильные приложения. Реквизиты карты	Характеризует системы защиты платежей и данных. Объясняет

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
	цифровой среде		и коды подтверждения. Системы защиты платежей и данных. Роль биометрии и её уязвимость перед подделкой голоса. Типовые схемы атак на семейный бюджет.	роль биометрии и её уязвимость. Выявляет типовые схемы атак на семейный бюджет.
23	Вредоносное программное обеспечение и современные средства защиты	1	Виды вредоносного ПО. Пути распространения и признаки заражения. Как работает антивирус. Роль машинного обучения. Обновления и резервное копирование. ИИ на стороне атакующих. Безопасная загрузка программ. Таргетированные атаки на критическую инфраструктуру.	Классифицирует вредоносное ПО. Называет пути распространения и признаки заражения. Объясняет принцип действия антивируса и роль машинного обучения. Соблюдает правила безопасной загрузки.
24	Искусственный интеллект в промышленности и сельском хозяйстве: автоматизация и безопасность	1	Компьютерное зрение для контроля качества, роботизированные линии, умное сельское хозяйство и транспорт. Что остаётся человеку. Чем «умнее» производство, тем оно уязвимее для информационных атак. Защита критической инфраструктуры.	Характеризует задачи ИИ на производстве. Объясняет, почему «умное» производство уязвимее для атак. Называет меры защиты критической инфраструктуры.
25	ИИ в авиации, космосе и беспилотных системах. Защита каналов связи	1	Применение ИИ в космосе: распознавание снимков, планирование миссий, поиск сигналов. Канал «Земля — борт — Земля», задержка сигнала. Угрозы: перехват, подмена команд и телеметрии, компрометация наземного сегмента.	Анализирует примеры применения ИИ в космосе. Описывает канал связи и последствия задержки сигнала. Характеризует угрозы передачи данных и принципы защиты.
26	Профессии на стыке ИИ и информационной безопасности: требования и траектории	1	Профессии цикла данных и ИИ. Профессии информационной безопасности: специалист по защите информации, аналитик центра мониторинга, тестировщик на проникновение. Востребованные школьные знания. Индивидуальная траектория: профильные предметы, олимпиады, ОГЭ по информатике, проекты и курсы.	Перечисляет профессии цикла данных и ИИ, а также профессии ИБ. Описывает их задачи. Соотносит задачи профессии со школьными знаниями. Характеризует индивидуальную траекторию.
27	Личный регламент работы с ИИ и базовые правила	1	Личный «паспорт безопасности» и регламент работы с ИИ-сервисами.	Повторяет изученный материал. Собирает личный «паспорт безопасности» и регламент

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
	информационной безопасности		Итоги: «ИИ — это…», «ИИ умеет…», «в нём нельзя…», «как я себя берегу». Ключевое правило: совет даёт ИИ, решает человек.	работы с ИИ. Формулирует обобщающие суждения и правило безопасности.
Итого		**27**		

8–9 КЛАССЫ (27 Ч.)

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
1	Искусственный интеллект: какие задачи он решает и где ошибается	1	Задачи, которые ИИ решает на уровне человека. Отличие обучаемой модели от обычной программы. Границы применимости. Ключевое правило: совет даёт ИИ, решение и ответственность — за человеком.	Объясняет отличие обучаемой модели от обычной программы. Характеризует границы применимости. Формулирует ключевое правило.
2	Эволюция идей искусственного интеллекта: от логических правил к обучению на данных	1	Символический ИИ, экспертные системы, статистическое обучение, генеративные алгоритмы, ИИ-агенты. Роль данных и вычислительных мощностей. Контроль человека. Отечественная микроэлектроника и центры обработки данных.	Описывает основные этапы развития ИИ. Анализирует роль данных и мощностей. Характеризует новые риски и необходимость контроля человека.
3	Вклад отечественных учёных в развитие искусственного интеллекта	1	Помощь ИИ науке. Учёные: 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.	Характеризует вклад отечественных учёных. Приводит примеры использования ИИ в науке. Работает с ресурсами сети для сбора сведений.
4	Как устроена искусственная нейронная сеть: от формального нейрона к обучаемой модели	1	Мозг и нейрон как источник аналогии. Математическая модель нейрона. Статистический характер вывода. Как отличить рассуждение человека от ответа ИИ. Уточняющие	Характеризует статистический характер вывода. Формулирует уточняющие запросы. Отличает рассуждение человека от ответа ИИ.

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
			запросы.	
5	Достоверность информации и методы её проверки: факт, оценка, источник	1	Факт, оценка и мнение. Критерии достоверности и актуальности. Перекрёстная проверка. Культурное и мировоззренческое содержание ответов ИИ. Признаки сфабрикованной информации. Проверка изображений, ссылок и метаданных. «Галлюцинации» ИИ.	Разграничивает факт, оценку и мнение. Применяет критерии достоверности. Проверяет метаданные и водяные знаки. Оценивает ответ нейросети как источник.
6	От научной фантастики к инженерии: какими представляли умные машины и что стало технологией	1	Образ «думающей машины» в литературе, кино и искусстве. Что сбылось, что осталось метафорой. «Восставший робот» — сюжетный приём. Реальные риски: слежка, дезинформация, манипуляция, утрата контроля.	Соотносит образ «думающей машины» с современными технологиями. Объясняет разницу между сюжетным приёмом и реальными рисками. Характеризует реальные угрозы.
7	Этика и правовое регулирование искусственного интеллекта	1	Этические принципы ИИ: справедливость, прозрачность, объяснимость, безопасность, подотчётность. Права человека в среде ИИ-сервисов. Защита от дискриминации алгоритмами. Право на объяснение. Принцип «человек принимает решение».	Называет этические принципы ИИ. Характеризует права человека в среде ИИ-сервисов. Обосновывает принцип «человек принимает решение».
8	Социальная инженерия: как обманывают не компьютер, а человека	1	Психологические приёмы: дефицит времени, страх, лесть, авторитет, жадность. Типовые сценарии. Вербовка подростков. «Несложные поручения» как вовлечение в уголовно наказуемую деятельность. Как ИИ усиливает манипуляцию. Личный алгоритм защиты.	Описывает психологические приёмы обмана. Характеризует типовые сценарии. Применяет личный алгоритм: пауза, проверка по независимому каналу, отказ называть код и персональные данные.
9	ИИ в повседневных цифровых сервисах: принципы работы, настройки, приватность	1	Поисковая выдача, рекомендации, переводчики, распознавание речи, автодополнение, навигация, голосовые помощники. Обучаемая модель и её зависимость от данных пользователя. Настройки приватности и разрешения приложений.	Анализирует принципы работы привычных сервисов. Объясняет зависимость модели от данных пользователя. Ограничивает сбор данных настройками.
10	Аутентификация и защита доступа	1	Пароль как ключ доступа. Длина пароля, алфавит и число комбинаций. Менеджеры	Объясняет связь длины пароля и числа комбинаций. Различает факторы аутентификации.

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
			паролей, двухфакторная аутентификация, одноразовые коды. Биометрия и аппаратные ключи. Уникальность пароля. Проверка утечек, аудит cookie и трекеров. «Угон» через код из СМС. Как ИИ помогает атакующим.	Обосновывает требования к стойкости и уникальности пароля. Настраивает двухфакторную защиту.
11	Безопасное общение в цифровой среде: сетевой этикет, анонимность, верификация собеседника	1	Сетевой этикет. Кибербуллинг и противодействие. Правовые последствия травли и распространения личной информации. Горячие линии. Принцип «по другую сторону экрана может быть человек и ИИ-агент». Верификация собеседника. Признаки опасных знакомств. Защита устройства и аккаунтов.	Понимает, что по переписке нельзя надёжно установить личность. Применяет правила проверки. Характеризует способы противодействия кибербуллингу. Верифицирует собеседника.
12	Компьютерное распознавание изображений, речи и текста: признаки, модели, ошибки	1	Дискретное представление изображений и звука. Распознавание речи и синтез голоса. Оптическое распознавание текста. Компьютерное зрение. Генерация изображений по описанию. Трудности распознавания. Риск слежки и этические ограничения биометрии.	Объясняет принцип компьютерного восприятия через дискретное представление данных. Характеризует задачи распознавания и типичные ошибки. Оценивает риски слежки.
13	Персональные данные, цифровой след и цифровая репутация	1	Персональные данные и их защита. Права субъекта данных. Цифровой след: cookie, метаданные, публикации, геолокация. Как ИИ связывает данные в профиль. Управление цифровой репутацией. Правила обращения с данными при учебных заданиях.	Раскрывает, что относится к персональным данным. Характеризует цифровой след. Объясняет, как ИИ связывает данные в профиль. Управляет цифровой репутацией.
14	Согласия, настройки приватности и профилирование: кто и как собирает данные	1	Пользовательские соглашения, политики конфиденциальности, cookie-уведомления. Разрешения приложений. Профилирование и персонализация рекламы. Как данные питают ИИ-рекомендации. Как ИИ-системы ищут жертв мошенничества.	Читает соглашения и политики конфиденциальности. Настраивает разрешения приложений. Характеризует профилирование и персонализацию рекламы.
15	Промышленный и бытовой интернет	1	Бытовой и промышленный Интернет вещей. Сбор данных	Описывает контур «датчик — сигнал — решение —

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
	вещей в умном городе: автоматизация, обратная связь, большие данные		с датчиков и принятие решений. Безопасность Интернета вещей: пароли по умолчанию, уязвимые прошивки, открытые сети. Защита домашней сети. Большие данные и граница приватности.	исполнитель». Анализирует пользу больших данных и границу приватности. Характеризует типовые уязвимости IoT.
16	Цифровые двойники	1	Цифровой двойник как компьютерная модель объекта. Роль ИИ в калибровке и прогнозировании. Риски: чувствительность данных двойника, возможность использовать копию против оригинала.	Раскрывает смысл понятия «цифровой двойник». Характеризует роль ИИ в калибровке и прогнозировании. Оценивает риски использования копии против оригинала.
17	Синтетические медиа: дипфейки и методы их обнаружения	1	Генерация реалистичных видео, аудио и изображений. Признаки подделки: артефакты, несогласованность мимики, метаданные, водяные знаки, отсутствие подтверждения. ИИ на стороне подделки и защиты. Регламент проверки.	Объясняет принцип генерации реалистичных медиа. Выявляет признаки подделки. Применяет регламент «не верь глазам — проверь источник, уточни у адресата, не сообщай коды».
18	Онлайн-мошенничество: технические и социальные механизмы, действия после инцидента	1	Фишинговые письма и ссылки, фальшивые конкурсы, поддельные службы поддержки, мошенничество с картами. ИИ усиливает приманки. Алгоритм действий после обмана. Подача заявления через электронную приёмную МВД. Доказательства. Последствия участия подростков в мошенничестве.	Классифицирует типовые схемы. Объясняет, как ИИ усиливает приманки. Характеризует алгоритм действий после инцидента: зафиксировать доказательства, сменить пароли, сообщить взрослым, обратиться в поддержку и полицию.
19	Нейросеть как инструмент обучения, а не замена мышлению: академическая честность	1	Роль ИИ в учебной работе. Приёмы формулирования запроса. Обязательная проверка результата. Распознавание ошибок модели. Ссылка на источник и авторство идеи. Правила честности. «Ручная» проверка ссылок, документов, цитат и статистических данных.	Демонстрирует последовательность: самостоятельная попытка, фиксация затруднения, ограниченная подсказка, проверка, объяснение решения. Соблюдает академическую честность.
20	Генеративный ИИ и авторское право: кто автор созданного ИИ произведения	1	Генерация текста, изображений и музыки. ИИ — инструмент, творческий этап остаётся за человеком. Правовой статус сгенерированного контента.	Объясняет принцип генерации. Различает правовой статус сгенерированного контента. Отмечает работу, выполненную с помощью ИИ. Ответственно

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
			Авторское право, права на изображение и голос. Договоры с сервисами. Маркировка ИИ-контента. Этика использования.	относится к чужому труду.
21	ИИ на службе медицины: задачи диагностики, ограничения, ответственность	1	Распознавание медицинских изображений и сигналов. ИИ как «второй взгляд», но не замена врача. Ответственность врача. Опасность самолечения. Фитнес-устройства и рекомендации. Безопасность передачи медицинских данных и настройка доступа.	Характеризует задачи компьютерного распознавания медицинских изображений. Объясняет, почему ИИ не заменяет врача. Оценивает качество модели через цену ошибок. Называет медицинские данные особо чувствительными.
22	Безопасность финансовых средств в цифровой среде	1	Онлайн-банкинг и мобильные приложения. Реквизиты карты и коды подтверждения. Системы защиты платежей и данных. Роль биометрии и её уязвимость перед подделкой голоса. Типовые схемы атак на семейный бюджет.	Характеризует системы защиты платежей и данных. Объясняет роль биометрии и её уязвимость. Выявляет типовые схемы атак на семейный бюджет.
23	Вредоносное программное обеспечение и современные средства защиты	1	Виды вредоносного ПО. Пути распространения и признаки заражения. Как работает антивирус. Роль машинного обучения. Обновления и резервное копирование. ИИ на стороне атакующих. Безопасная загрузка программ. Таргетированные атаки на критическую инфраструктуру.	Классифицирует вредоносное ПО. Называет пути распространения и признаки заражения. Объясняет принцип действия антивируса и роль машинного обучения. Соблюдает правила безопасной загрузки.
24	Искусственный интеллект в промышленности и сельском хозяйстве: автоматизация и безопасность	1	Компьютерное зрение для контроля качества, роботизированные линии, умное сельское хозяйство и транспорт. Что остаётся человеку. Чем «умнее» производство, тем оно уязвимее для информационных атак. Защита критической инфраструктуры.	Характеризует задачи ИИ на производстве. Объясняет, почему «умное» производство уязвимее для атак. Называет меры защиты критической инфраструктуры.
25	ИИ в авиации, космосе и беспилотных системах. Защита каналов связи	1	Применение ИИ в космосе: распознавание снимков, планирование миссий, поиск сигналов. Канал «Земля — борт — Земля», задержка сигнала. Угрозы: перехват, подмена команд и телеметрии, компрометация наземного сегмента.	Анализирует примеры применения ИИ в космосе. Описывает канал связи и последствия задержки сигнала. Характеризует угрозы передачи данных и принципы защиты.

№ п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
26	Профессии на стыке ИИ и информационной безопасности: требования и траектории	1	Профессии цикла данных и ИИ. Профессии информационной безопасности: специалист по защите информации, аналитик центра мониторинга, тестировщик на проникновение. Востребованные школьные знания. Индивидуальная траектория: профильные предметы, олимпиады, ОГЭ по информатике, проекты и курсы.	Перечисляет профессии цикла данных и ИИ, а также профессии ИБ. Описывает их задачи. Соотносит задачи профессии со школьными знаниями. Характеризует индивидуальную траекторию.
27	Личный регламент работы с ИИ и базовые правила информационной безопасности	1	Личный «паспорт безопасности» и регламент работы с ИИ-сервисами. Итоги: «ИИ — это…», «ИИ умеет…», «в нём нельзя…», «как я себя берегу». Ключевое правило: совет даёт ИИ, решает человек.	Повторяет изученный материал. Собирает личный «паспорт безопасности» и регламент работы с ИИ. Формулирует обобщающие суждения и правило безопасности.
Итого		**27**		