МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНПРОСВЕЩЕНИЯ РОССИИ)

Департамент государственной общеобразовательной политики и развития дошкольного образования

Люсиновская ул., д. 51, Москва, 115093
Тел. (495) 587-01-10, доб. 3250
E-mail: d03@edu.gov.ru

03.11.2026 № 03-2249

Руководителям исполнительных органов субъектов Российской Федерации, осуществляющих государственное управление в сфере образования

О содержании программ внеурочной деятельности

Уважаемые коллеги!

Департамент государственной общеобразовательной политики и развития дошкольного образования Минпросвещения России (далее – Департамент) направляет рабочие программы курса внеурочной деятельности «Искусственный интеллект и информационная безопасность» (далее – программы) для уровней основного общего и среднего общего образования, а также инструктивно-методическое письмо о содержании программ, планируемых к реализации в режиме апробации с 11 ноября 2026 года.

Департамент просит довести информацию до муниципальных органов управления образованием, образовательных организаций, всех заинтересованных лиц.

Приложение: в электронном виде.

Исполняющий обязанности директора Департамента

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат BC3B7E5C410653D35315CCD7734865E5FC601FBA
Владелец Поляков Илья Сергеевич
Действителен с 27.02.2026 по 23.05.2027
Подписник электронного документа, подписанного электронной подписью, хранится в единой системе электронного документооборота Министерства просвещения Российской Федерации

И.С. Поляков

Бахмет Ю.П.
(495) 587-01-10, доб. 3257

Приложение

О содержании программ курса внеурочной деятельности «Искусственный интеллект и информационная безопасность»

В соответствии с федеральными государственными образовательными стандартами основного общего и среднего общего образования программы основного общего и среднего общего образования реализуются общеобразовательными организациями через организацию образовательной деятельности (урочной и внеурочной).

Внеурочная деятельность является неотъемлемой и обязательной частью образовательного процесса. Она организуется в целях обеспечения индивидуальных потребностей обучающихся и осуществляется в формах, отличных от урочных.

С 2026/2027 учебного года и далее 1 час в неделю из возможных 10 часов внеурочной деятельности для учащихся 5-9 и 10-11 классов рекомендуется отводить на внеурочные занятия курса «Искусственный интеллект
и информационная безопасность» (далее – курс).

Курс направлен на формирование у обучающихся 5-9 и 10-11 классов целостного и реалистичного представления об искусственном интеллекте (далее – ИИ) как о междисциплинарном инструменте-помощнике, обеспечение системного расширения знаний о его работе, роли в науке, экологии, медицине, образовании и промышленности, а также закрепление теории практическим опытом взаимодействия с доступными ИИ-технологиями.

Содержание и результаты курса разработаны с опорой на Стратегию научно-технологического развития Российской Федерации (Указ Президента Российской Федерации от 28 февраля 2024 г. № 145), Национальную стратегию развития искусственного интеллекта на период до 2030 года (Указ Президента Российской Федерации от 10 октября 2019 г. № 490) и федеральный проект «Искусственный интеллект», входящий в национальный проект «Экономика данных и цифровая трансформация государства».

Рабочие программы курса разработаны ФГБНУ «Институт содержания и методов обучения имени В.С. Леднева» и доступны на портале Единого содержания общего образования по адресу: https://edsoo.ru/rabochie-programmy-vd/.

Рабочие программы курса содержат тематическое планирование, дифференцирующее как предметные результаты, так и предметное содержание по годам изучения.

Содержание рабочих программ выстроено вокруг единой сквозной идеи: совет дает искусственный интеллект, а решение и ответственность остаются за человеком. Это правило определяет и содержание занятий и формулировки планируемых результатов. Педагогу надлежит последовательно раскрывать обучающимся, что ответ ИИ-модели не обладает самостоятельным моральным авторитетом, а перекладывание ответственности за собственные решения на алгоритм или сервис неприемлемо.

Курс имеет две равноправные содержательные линии, идущие параллельно на всех уровнях обучения:

1) линия искусственного интеллекта – понятие и сущность искусственного интеллекта, история и эволюция идей, вклад отечественной научной школы, устройство и границы применимости нейронных сетей и больших языковых моделей, компьютерное восприятие, генеративные технологии, применение ИИ в отраслях и профессиях;

2) линия информационной безопасности – персональные данные и цифровой след, аутентификация и защита доступа, социальная инженерия и онлайн-мошенничество, вредоносное программное обеспечение и средства защиты, достоверность информации и синтетические медиа (дипфейки), безопасность интернета вещей и критической информационной инфраструктуры, этические и правовые нормы использования ИИ. Каждое занятие объединяет обе линии либо акцентирует одну из них.

Содержание курса усложняется по концентрическому принципу в трех группах классов (5-7, 8-9, 10-11 классы). Преемственность между группами классов обеспечивается не повторением тем, а глубиной их раскрытия и характером учебной деятельности.

Организационная схема подготовки и введения курса (рис. 1) представляет собой строгую вертикально-ориентированную многоуровневую структуру.

Федеральным оператором введения курса выступает Федеральное государственное бюджетное научное учреждение «Институт изучения детства, семьи и воспитания». Федеральный оператор готовит учебно-методическое обеспечение для реализации курса.

Через инструктивные письма управление передается на региональный уровень. Органом исполнительной власти субъекта Российской Федерации, осуществляющим государственное управление в сфере образования,

назначен региональный координатор – лицо, ответственное за введение курса в субъекте Российской Федерации, а также (рекомендуется) организация-оператор введения курса (как правило, региональный институт развития образования (далее – ИРО). Назначенный региональный координатор и ИРО проводят инвентаризацию готовности образовательных организаций к введению курса, организуют работу с муниципальными органами управления образованием и сопровождение педагогов. Силами организации-оператора создана служба межшкольных тьюторов, которая осуществляет сбор и обобщение сложных вопросов, связанных с введением курса, и оказывает содействие в их разрешении.

На уровне общеобразовательной организации руководитель принимает необходимые локальные нормативные акты, утверждает расписание и обеспечивает инфраструктуру для реализации курса. Педагоги, ответственные за реализацию курса, непосредственно проводят занятия внеурочной деятельности по готовым сценариям и используют готовые учебно-методические материалы.

Проведение внеурочной деятельности тарифицируется и оплачивается. При кадровом дефиците задействуется сетевая форма реализации образовательной программы: к реализации курса могут быть привлечены работники центров дополнительного образования детей «Кванториум», центров цифрового образования детей «IT-куб» и центров образования цифрового и гуманитарного профилей «Точка роста», созданных непосредственно на базе общеобразовательных организаций, либо расположенных неподалеку.

Организационная схема предусматривает двусторонние информационные потоки (от общеобразовательных организаций и муниципалитетов к регионам, далее к федеральному оператору и обратно), что обеспечивает непрерывный мониторинг, обратную связь и корректировку на всех этапах введения курса.



Рисунок 1. Организационная схема подготовки и введения курса



Федеральное государственное бюджетное научное учреждение «Институт содержания и методов обучения им. В.С. Леднева»

Рабочая программа курса внеурочной деятельности

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

(среднее общее образование)

Москва
2026

СОДЕРЖАНИЕ

Пояснительная записка 3
Содержание курса внеурочной деятельности 7
«Искусственный интеллект и информационная безопасность» 7
Планируемые результаты освоения программы 15
курса внеурочной деятельности 15
«Искусственный интеллект и информационная безопасность» 15
Личностные результаты 15
Метапредметные результаты 18
Предметные результаты 22
Тематическое планирование 26

Пояснительная записка

Программа курса внеурочной деятельности «Искусственный интеллект и информационная безопасность» для 10–11 классов интегрирует знания различных предметных областей и 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. На уровне среднего общего образования программа выходит за пределы знакомства с отдельными сервисами и переходит к системному анализу технологий: обучающиеся рассматривают, как устроены обучаемые большие языковые модели и какие границы их применимости, как обеспечивается защита информации на уровне механизмов, а не только рекомендаций, и как правовые и этические нормы ограничивают использование искусственного интеллекта (далее – ИИ). Программа способствует формированию цифровой 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 (далее – ИБ).

Содержание программы выстроено вокруг сквозной идеи: совет дает ИИ, а решение и ответственность остаются за человеком. Здесь раскрываются обучаемость и переобучение нейронных сетей, статистическая природа генерации текста, криптографические основы аутентификации, правовой режим персональных данных, этика и право в сфере ИИ, а также прикладные области (медицина, промышленность, космические системы и др.), где цена ошибки модели и требования к ее верификации максимальны.

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

- приоритеты и перспективы, обозначенные в Стратегии научно-технологического развития Российской Федерации (утверждена Указом Президента Российской Федерации от 28.02.2024 № 145);
- требования информационного общества, инновационной экономики и научно-технологического развития;
- Национальную стратегию развития искусственного интеллекта на период до 2030 года (утв. Указом Президента Российской Федерации от 10.10.2019 № 490);
- 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 основным 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. Для обучающихся 10–11 классов этот блок приобретает дополнительное значение: содержание курса связано с профессиональным самоопределением и показывает траектории входа в профессии на стыке ИИ и информационной безопасности.

Программа знакомит обучающихся с устройством и возможностями современных технологий искусственного интеллекта: с эволюцией ИИ от символьных систем к большим языковым моделям и автономным агентам, с основами нейронных сетей и вероятностной природой их работы, с компьютерным восприятием и генерацией изображений, речи и текста. Рядом с линией ИИ проходит линия информационной безопасности: обучающиеся рассматривают оценку достоверности информации в эпоху генеративного ИИ, социальную инженерию, аутентификацию и криптографические основы защиты доступа, персональные данные и цифровой след, согласия и профилирование, синтетические медиа и дипфейки, вредоносное программное обеспечение и средства защиты. Отдельный блок посвящен этическим и правовым нормам: предвзятости алгоритмов, ответственности за автоматизированное решение, авторству сгенерированного контента, границам применения ИИ в медицине, промышленности и космических системах. Обучающиеся учатся формулировать запрос, критически оценивать вывод большой языковой модели, проверять факты и код по независимым источникам, настраивать приватность в типовых сервисах и применять изученные правила для защиты себя и своей информации в цифровой среде.

Программа конкретизирует содержание, планируемые предметные, метапредметные и личностные результаты. Стратегическими документами, определяющими содержание и результаты обучения, являются федеральный государственный образовательный стандарт среднего общего образования, утверждённый приказом Минпросвещения России от 17.05.2012 № 413 и соответствующая федеральная образовательная программа среднего общего образования, утвержденная приказом Минпросвещения России от 18.05.2023 № 371.

Основной целью освоения содержания программы является получение обучающимися знаний, умений и навыков в сфере искусственного интеллекта и информационной безопасности – перспективной области информационных и коммуникационных технологий; формирование и развитие компетенций

обучающихся в области применения ИКТ и технологий искусственного интеллекта; работы с информацией, представленной различными знаковыми средствами и образными формами, критического отношения к информации; коммуникации в цифровом пространстве с применением правил информационной безопасности; воспитания ответственного отношения к информации с учетом правовых и этических норм ее использования и распространения, стремления к продолжению образования в сфере искусственного интеллекта и созидательной деятельности с применением средств ИИ-технологий.

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 понимания вероятностной природы обучаемых моделей, границ их применимости и необходимости верификации результата по независимым источникам;

– 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, основ работы с данными, коммуникации на современных цифровых платформах, информационной безопасности; воспитание критического отношения к информации с учетом правовых и этических норм ее использования, распространения и генерирования;

– знакомство с профессиями на стыке ИИ и информационной безопасности, требованиями к ним и траекториями профессионального входа.

Обучение учащихся в сфере искусственного интеллекта и информационной безопасности носит интегративный и практико-ориентированный 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.

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.).

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. Программа учитывает задачи профильного обучения и ориентирует обучающихся на выбор профильных предметов (информатика, математика), планирование личной образовательной траектории с учётом требований ЕГЭ и возможность поступления на ИТ-направления в вузы и колледжи.

Содержание курса внеурочной деятельности «Искусственный интеллект и информационная безопасность»

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 большой языковой модели от обычной программы: результат формируется на основе обработки больших данных, а не задается жесткой инструкцией. Границы применимости: почему модель, хорошо решающая одну задачу, беспомощна в другой. Ключевое правило безопасного применения ИИ: совет дает ИИ, а решение и ответственность – за человеком.

Занятие 2. Эволюция искусственного интеллекта: от символического ИИ к большим языковым моделям

Символический ИИ и экспертные системы, статистическое машинное обучение, глубокое обучение нейронных сетей, трансформеры и большие языковые модели, автономные ИИ-агенты. Движущие факторы развития ИИ. Чем автономнее система, тем выше цена ее ошибки: необходимость верифицируемости, прозрачности и защиты обрабатываемой информации. Перспективы развития отечественной микроэлектроники и центров обработки данных.

Занятие 3. Отечественная научная школа и развитие искусственного интеллекта

Вклад отечественных ученых в становление 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. Современные достижения российской науки и техники в области ИИ, уникальные условия России для ее технологического лидерства.

Исторический и этический контекст: дискуссия о кибернетике в СССР и уроки отношения общества к новым технологиям. Роль отечественных разработок в обеспечении технологического суверенитета. Важность создания собственных вычислительных мощностей, инструментов и наборов данных для обучения моделей ИИ в условиях внешних ограничений.

Занятие 4. Основы нейронных сетей: от модели нейрона к большой языковой модели

Формальный нейрон. Идея обучения нейросетей. Почему обучение на данных не равно пониманию: обобщающая способность, переобучение, роль объема и качества обучающей выборки. Статистические методы в основе генерации текста.

Занятие 5. Экспертиза информации в эпоху генеративного ИИ

Алгоритм оценки источника: первичные и вторичные данные, библиографическая и фактологическая проверка, работа с метаданными и обратным поиском изображений. Когнитивные искажения и манипулятивные техники в подаче информации. Ответственность за репост и производство контента. Специфические ошибки генеративных алгоритмов в составе больших языковых моделей: «галлюцинации», правдоподобная недостоверность; практика верификации ответов ИИ по независимым источникам.

Занятие 6. Образ искусственного разума в культуре: от прогноза к инженерной реальности

Эволюция представлений об ИИ в литературе, кино и искусстве и их влияние на общественные ожидания и на сами исследования. Разграничение научной фантастики, футурологического прогноза и реальной технологической траектории. Почему ожидания регулярно расходятся с реальностью. Реальные, а не сюжетные риски ИИ: концентрация данных и вычислительных ресурсов, манипуляция, утрата контроля над автономными системами.

Занятие 7. Этика и право в сфере искусственного интеллекта

Ключевые этические проблемы: предвзятость алгоритмов и справедливость, прозрачность и объяснимость, ответственность за решение, приватность. Права человека в цифровой среде: право на объяснение автоматизированного решения, защита от дискриминации, значимые решения – только при участии человека.

Занятие 8. Социальная инженерия и принцип нулевого доверия: противодействием атаке

Атака через доверие: разведка цели, подготовка легенды, канал воздействия, момент действия. Почему человек – «слабое звено» защиты. Вовлечение подростков в уголовно наказуемую деятельность: дропперство, «работа курьером», передача/приём денег, ложные сообщения о минировании по заданию «куратора», вербовка в мессенджерах и онлайн-играх.

ИИ как инструмент атакующего: клонирование голоса и лица, генерация убедительных текстов и автоматизация целевого фишинга. Регламенты подтверждения операций, правило «нулевого доверия» к просьбам о данных и деньгах, культура сообщения об инцидентах. Правовые последствия действий подростков в сети с позиции уголовной ответственности: статья 159 УК РФ (мошенничество) и статья 159.6 УК РФ (мошенничество в сфере компьютерной информации), предусматривающие ответственность за

хищение путём обмана или доверия, в том числе через воздействие на компьютерную информацию, с максимальным наказанием до десяти лет лишения свободы, статья 272 УК РФ – неправомерный доступ к охраняемой компьютерной информации.

Занятие 9. Сервисы на основе ИИ: устройство, экономика данных и приватность

Как устроены рекомендательные и поисковые сервисы, переводчики, голосовые ассистенты. Экономика данных: «бесплатный» сервис, монетизация поведенческих данных, клиент-серверная архитектура. Управление приватностью: разрешения приложений, настройки рекламных профилей, минимизация оставляемых данных.

Занятие 10. Аутентификация и защита доступа: от пароля к многофакторным схемам

Криптографические основы пароля: пространство ключей и трудоемкость перебора, почему важна стойкость и уникальность. Многофакторная и адаптивная аутентификация: одноразовые коды, аппаратные ключи, биометрия и PUSH-подтверждения, менеджер паролей. Настройка двухфакторной аутентификации на учебном аккаунте, проверка стойкости паролей через открытые сервисы оценки сложности, примеры утечки паролей. Атаки нового типа: подбор по базам утечек, генеративный фишинг и клонирование голоса. Противодействие на уровне человека и устройств.

Занятие 11. Коммуникации в цифровой среде: этикет, анонимность, доверие и травля

Сетевой этикет и правовые рамки общения. Анонимность, верификация личности собеседника и проблема доверия в открытых каналах. ИИ-собеседники: чат-боты и ИИ-агенты в переписке и играх.

Кибербуллинг: психология, правовые последствия, алгоритмы безопасного поведения и поддержки пострадавших.

Действия при травле в сети. Признаки вовлечения в деструктивные сообщества, алгоритм действий при получении угроз или призывов, координаты горячих линий. Правовые последствия действий подростков в сети с позиции уголовной ответственности: статья 137 УК РФ (нарушение неприкосновенности частной жизни) и статья 137.1 (распространение персональных данных), а также статьи 110, 110.1 и 110.2 – доведение до самоубийства, склонение к нему и организация деятельности, побуждающей к нему, статья 128.1 (клевета) применима к распространению заведомо ложных сведений в сети.

Занятие 12. Компьютерное восприятие: распознавание изображений, речи и текста

Как компьютер «видит» датчиками: 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 правовые основы их защиты

Правовое содержание понятия персональных данных: категории, основания и цели обработки, права субъекта и обязанности оператора. Цифровой след и профиль: cookie и метаданные, геолокация, поведенческие данные. Как ИИ собирает разрозненные сигналы в узнаваемый профиль. Цифровая репутация и самопрезентация в сети. Управление приватностью, удаление и переносимость данных.

Правовые последствия действий подростков в сети с позиции уголовной ответственности: статья 272.1 УК РФ – незаконные использование, сбор и хранение компьютерной информации, содержащей персональные данные, с усиленной ответственностью при работе с данными несовершеннолетних и биометрией.

Занятие 14. Согласия, настройки приватности и профилирование: как устроен сбор данных

Правовой смысл согласий и политик конфиденциальности, cookie-уведомления. Что искать в тексте и какие права он ограничивает. Разрешения приложений, профилирование рекламы. Манипулятивные интерфейсы, побуждающие к опасным действиям. Практика настройки приватности в типовых сервисах. Настройки приватности: аудит разрешений установленных приложений на смартфоне с отзывом избыточных разрешений на камеру, микрофон, геолокацию и контакты, настройку cookie в браузере; чтение типового пользовательского соглашения с поиском ключевых пунктов о передаче данных третьим лицам, праве на удаление и юрисдикции.

Занятие 15. Интернет вещей и умный город: автоматизация, обратная связь и большие данные

Архитектура умного города: сеть датчиков и исполнителей, контур управления с обратной связью. Большие данные и анализ в интересах города: транспорт, ЖКХ, безопасность. Где проходит граница между эффективностью и приватностью при массовом сборе данных. Специфика защищенности: слабые пароли по умолчанию, безопасность беспроводных каналов.

Занятие 16. Цифровые двойники и компьютерное моделирование

От информационных и имитационных моделей к цифровому двойнику. Роль ИИ в двойниках: калибровка параметров, обучение на данных, прогноз состояний и сценарное тестирование без риска для реального объекта. Риски и ответственность: чувствительность данных двойника, последствия неточной модели, вопрос доверия к решениям, принятым на основе модели.

Занятие 17. Синтетические медиа: дипфейки и технологии противодействия

Технологии генерации синтетического контента: архитектуры и обучение, массовость и удешевление подделок аудио, видео и изображений. Методы выявления подделок: анализ артефактов и физиологических сигналов, метаданные и цифровые водяные знаки. ИИ на двух сторонах противостояния. Гигиена достоверности: верификация источника и перепроверка по независимому каналу.

Занятие 18. Онлайн-мошенничество: схемы, механизмы и порядок действий при инциденте

Классификация мошеннических схем: фишинг и клонирование сайтов, финансовое и игровое мошенничество. Психологические рычаги воздействия. ИИ как усилитель мошенничества: качество языка, персонализация, имитация голоса и видео, автоматизация массовых и точечных атак.

Клонирование голоса из открытых источников. «Голосовое подтверждение» как этап сбора биометрии. Дипфейк-видеозвонок от «значимого взрослого». Фейковое видео с участием известных личностей.

Регламент реагирования: фиксация доказательств, блокировка и смена учетных данных, уведомление банка, поддержки сервиса и правоохранительных органов. 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, какие сервисы самозащиты доступны на портале Госуслуг (проверка подозрительного номера, самозапрет на кредиты, проверка кредитной истории). Возможные последствия личного участия в мошенничестве (статья 159 УК РФ).

Занятие 19. ИИ в учебной деятельности: инструменты и честность

ИИ-инструменты в учебе и труде: объяснение и систематизация материала, генерация задач и тестов, редактура, границы допустимого. Последовательность выполнения учебных заданий: самостоятельное выполнение без обращения к помощи генеративного ИИ; дополнение полученного результата с помощью возможностей ИИ; обобщение и проверка

полученных результатов. Академическая честность: ответственность автора, риск делегирования мышления технологиям ИИ.

Занятие 20. Генеративный ИИ и интеллектуальное право: вопрос авторства

Правовые режимы сгенерированного контента: объект и субъект авторского права, права на изображение и голос, лицензионные условия сервисов, маркировка ИИ-контента. Экономическая и этическая сторона: обучение моделей на чужом творчестве, справедливая компенсация авторов, ответственность за нарушение прав. Правовые последствия действий подростков в сети с позиции уголовной ответственности: нарушение авторских и смежных прав (ст. 146 УК РФ).

Занятие 21. ИИ в медицине: диагностика, метрики качества и ответственность

Компьютерное распознавание медицинских изображений и сигналов: задачи, данные, архитектуры. ИИ как «второе мнение» врача. Цена ложноположительного и ложноотрицательного диагноза. Ответственность и этика: врач всегда сам принимает решение. Как датчики и алгоритмы фитнес-устройства получают и интерпретируют показатели. Почему ИИ-совет не заменяет диагностику: риск гипердиагностики и самолечения. Безопасность медицинских данных здоровья: передача и хранение, доступ третьих сторон.

Занятие 22. Безопасность финансовых средств в цифровой среде: архитектура защиты и роль ИИ

Архитектура защиты безналичных платежей: клиент-серверная модель и разделение зон ответственности, шифрование канала, протоколы подтверждения, многофакторная аутентификация при проведении операций.

Биометрия в финансовом доступе, включая голосовую и поведенческую: требования к защищённости образцов биометрических данных (152-ФЗ) и правовые рамки дистанционного банковского обслуживания (161-ФЗ).

Атаки на финансовый доступ: целевой фишинг, клонирование голоса знакомого. Порядок действий и фиксации инцидента, ответственность сторон при компрометации.

Занятие 23. Вредоносное программное обеспечение и системы защиты

Семейства и тактики вредоносного ПО: вирусы, черви, трояны, шпионское и рекламное ПО. Защита: антивирус, межсетевой экран, контроль приложений, обновления, резервное копирование. ИИ в атаке и обороне. Безопасность загрузки и установки программ.

Проверка устройства антивирусом, настройка межсетевого экрана операционной системы, проверка статуса обновлений операционной системы

и браузера, анализ примеров фишинговых писем с поиском признаков подделки – адреса отправителя, ссылок, вложений, срочности просьбы. Правовые последствия действий подростков в сети с позиции уголовной ответственности: статья 273 УК РФ – создание, использование и распространение вредоносных программ.

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

Промышленный ИИ: компьютерное зрение, предиктивное обслуживание, робототехника и автономные системы (БПЛА, наземные платформы). Понятие периферийного ИИ для работы в условиях отсутствия связи. Защита критической информационной инфраструктуры от кибератак и «отравления данных». Человек в условиях автоматизации: изменение содержания труда, переквалификация, сохранение ответственности человека за критические решения.

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

Автономные и пилотируемые системы: где заканчивается «автопилот» и начинается ИИ. Предиктивное обслуживание техники по данным бортовых датчиков, компьютерное зрение для навигации и уклонения от препятствий, планирование миссий и анализ телеметрии и снимков, помощь диспетчеру и пилоту как «второе мнение». Почему в критических системах решение и ответственность остаются за человеком, а ИИ работает в контуре с обязательной верификацией. Канал связи как часть системы управления и как мишень: связь «земля – борт – земля», спутниковая и радионавигация, телеметрия и команды управления беспилотником. Регуляторные требования к кибербезопасности критической инфраструктуры и авиационных систем; этические и правовые вопросы применения беспилотников.

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

Профессии в индустрии ИИ и анализа данных: исследователь машинного обучения, инженер данных, аналитик, промпт-инженер, специалист по этике и качеству моделей, инженер по кибербезопасности промышленных систем, разработчик бортовых систем ИИ, специалист по цифровым двойникам, инженер-материаловед с компетенциями в науках о данных (Data Science). Акцент на междисциплинарность: важность физики, химии и математики наравне с программированием.

Профессии в информационной безопасности: аналитик, инженер по защите информации, специалист по реагированию на инциденты. Траектория «входа» в профессию: профильное обучение и ЕГЭ, олимпиады, ИТ-

специальности вузов и колледжей, портфолио проектов и соревнования. Дефицит и перспективы кадров.

«Нецифровые» профессии: расширение возможностей профессиональной деятельности учителя, врача, военного, спасателя и т.д. навыками в сфере ИИ для стабилизации социально-экономической ситуации на рынке труда.

Занятие 27. Личная стратегия работы с ИИ и информационной безопасности: итоговая рефлексия

Формирование персональной методики: с какими ИИ-сервисами работаю, для каких задач, как проверяю результат и что не доверяю модели. Формируем личную позицию «ИИ – это…», «он умеет…», «в нем нельзя…», «как я себя берегу». Закрепление главного принципа: совет дает ИИ, решает человек. План развития компетенций ИИ и ИБ после окончания школы.

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, 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:

– готовность участвовать в переходе к передовым цифровым, интеллектуальным, производственным технологиям, роботизированным системам, новым материалам и способам конструирования, созданию систем обработки больших объемов данных, машинного обучения и искусственного интеллекта;

– 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 – для планирования миссий;

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

– осознание важности морально-этических принципов в деятельности, связанной с реализацией технологий 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;

– 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.

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 ИИ-генерации 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;

– 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 и алгоритмических лент рекомендаций на самочувствие, внимание, 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

«Искусственный интеллект»:

– характеризовать вероятностную природу обучаемой большой языковой модели: объяснять, почему результат формируется на основе больших данных и не задается жесткой инструкцией, и почему вывод модели может быть ошибочным даже при правильном решении похожих задач;

– объяснять, почему модель, хорошо решающая одну задачу, беспомощна в решении другой, и в чем состоят переобучение, роль объема и качества выборки, обобщающая способность;

– раскрывать границы применимости больших языковых моделей;

– описывать эволюцию ИИ как смену парадигм от символьного ИИ и экспертных систем через статистическое машинное обучение и глубокое обучение нейронных сетей к трансформерам, большим языковым моделям и автономным ИИ-агентам и называть движущие факторы этого развития (данные, вычислительные мощности, алгоритмы);

– объяснять устройство формального нейрона и идею обучения сети как подбора весов по данным согласно критерию качества, а также статистическую природу генерации текста: почему обучение на данных не равно пониманию;

– характеризовать компьютерное восприятие на уровне принципов: дискретное представление изображений и звука, распознавание речи и синтез голоса, оптическое распознавание текста, компьютерное зрение, генерация изображений по описанию, а также причины трудностей распознавания (двусмысленность, ирония, шум в данных);

– раскрывать роль ИИ в системах с обратной связью и моделировании: от информационных и имитационных моделей к цифровому двойнику, где ИИ выполняет калибровку параметров, обучение на данных и прогнозирование состояний при сценарном тестировании без риска для реального объекта;

– анализировать применение ИИ в предметных областях с точки зрения цены ошибки и ответственности: медицина (метрики качества, ложноположительный и ложноотрицательный вывод, ИИ как «второе мнение»), промышленность и сельское хозяйство (компьютерное зрение, предиктивное обслуживание, робототехника), космические системы (автономная навигация, планирование миссий, связь «Земля – борт – Земля»);

– критически разграничивать научную фантастику, футурологический прогноз и реальную технологическую траекторию, противопоставляя сюжетным рискам реальные: концентрацию данных и вычислительных ресурсов, манипуляцию, утрату контроля над автономными системами.

«Информационная безопасность»:

– объяснять криптографические основы защиты доступа: связь пространства ключей и трудоемкости перебора со стойкостью и уникальностью пароля; различать однофакторную, многофакторную и адаптивную аутентификацию, обосновывать назначение одноразовых кодов, аппаратных ключей, биометрии, PUSH-подтверждений и менеджера паролей;

– раскрывать сценарии атак в социальной инженерии как последовательность «разведка цели – подготовка легенды – канал воздействия – момент действия» и объяснять, как ИИ усиливает ее на каждом шаге (клонирование голоса и лица, генерация убедительных текстов, автоматизация целевого фишинга);

– классифицировать схемы онлайн-мошенничества (фишинг, клонирование сайтов, финансовое и игровое мошенничество) и применять регламент реагирования на инцидент: фиксация доказательств, блокировка и смена учетных данных, уведомление банка, поддержки сервиса и правоохранительных органов;

– выявлять методы противодействия дипфейкам и синтетическим медиа (анализ артефактов и физиологических сигналов, метаданные,

цифровые водяные знаки), верифицировать источник и осуществлять перепроверку по независимому каналу;

– владеть алгоритмом экспертизы информации в эпоху генеративного ИИ: различать первичные и вторичные данные, применять библиографическую и фактологическую проверку, работу с метаданными и обратным поиском изображений, распознавать «галлюцинации» и правдоподобную недостоверность вывода модели;

– раскрывать правовое содержание понятия персональных данных: категории данных, основания и цели обработки, права субъекта и обязанности оператора; анализировать формирование цифрового следа и профиля как сбор ИИ разрозненных сигналов (cookie, метаданные, геолокация, поведенческие данные) в узнаваемый образ пользователя;

– оценивать специфику защищенности Интернета вещей и «умного» города: слабые пароли по умолчанию, безопасность беспроводных каналов, а также границы между эффективностью массового сбора данных и приватностью;

– объяснять правовой смысл согласий и политик конфиденциальности, cookie-уведомлений, читать их и находить существенные ограничивающие права пункты; распознавать манипулятивные интерфейсы, профилирование рекламы и управлять разрешениями и приватностью в типовых сервисах;

– классифицировать вредоносное ПО и объяснять многоуровневую защиту (антивирус, межсетевой экран, контроль приложений, обновления, резервное копирование), в том числе роль машинного обучения в обнаружении новых образцов.

«Практическая работа с ИИ-инструментами и учебная честность»:

– формулировать эффективный запрос к генеративной модели, выбирать режим и уточнения, критически оценивать полноту и корректность вывода, проверять полученные факты и код по независимым источникам и атрибутировать источник и авторство идеи;

– использовать ИИ как инструмент учебной и проектной деятельности (объяснение и систематизация материала, генерация задач и тестов, редактура), осознанно обозначая границы допустимого и не допуская делегирования ИИ собственного мышления;

– соблюдать правила академической честности: сначала решить самому, потом сверяться, не выдавать чужой результат за собственный; открыто указывать, какая часть результата получена с помощью ИИ;

– создавать с помощью генеративных моделей текст, изображение, аудио и видео, объясняя принцип генерации и разграничивая правовой статус сгенерированного контента: объект и субъект авторского права, права на изображение и голос, лицензионные условия сервисов, маркировку ИИ-контента;

– применять личную методику работы с ИИ-сервисами: определять, с какими сервисами и для каких задач работать, как проверять результат и какие задачи не доверять модели.

«Этика, право и профориентация»:

– анализировать ключевые этические проблемы ИИ: предвзятость алгоритмов и справедливость, прозрачность и объяснимость, ответственность за автоматизированное решение, приватность;

– раскрывать права человека в цифровой среде: право на объяснение автоматизированного решения, защиту от дискриминации алгоритмами, принцип «значимые решения только при участии человека»; характеризовать российское регулирование отношений в области ИИ и робототехники и федеральный проект «Искусственный интеллект»;

– описывать профессии на стыке ИИ и информационной безопасности (исследователь машинного обучения, инженер данных, аналитик, промпт-инженер, специалист по этике и качеству моделей; аналитик, инженер по защите информации, специалист по реагированию на инциденты), их задачи и востребованные знания;

– соотносить индивидуальную образовательную траекторию с требованиями ЕГЭ и профильными предметами, планировать вход в профессию через профильное обучение, олимпиады, ИТ-специальности вузов и колледжей, портфолио проектов;

– сформулировать и применять личную стратегию безопасной и честной работы с ИИ и закрепить главный принцип курса: совет дает ИИ, решает человек.

Тематическое планирование

№ / акцент занятия		Темы занятия[1]	Кол-во часов	Программное содержание	Характеристика деятельности обучающихся
1.	ИИ + ИБ	Искусственный интеллект: какие задачи он решает и где ошибается	1	Задачи, которые ИИ решает на уровне человека: распознавание образов и речи, генерация текста и изображений, планирование, игра. Отличие обучаемой большой языковой модели от обычной программы: результат формируется на основе обработки больших данных, а не задается жесткой инструкцией. Границы применимости: почему модель, хорошо решающая одну задачу, беспомощна в другой. Ключевое правило безопасного применения ИИ: совет дает ИИ, а решение и ответственность – за человеком.	Характеризовать задачи, которые ИИ решает на уровне человека: распознавание образов и речи, генерация текста и изображений, планирование, игра. Различать обучаемую модель и обычную программу: объяснять, что результат формируется на основе данных, а не задается жесткой инструкцией. Определять границы применимости модели и прогнозировать, когда надежный результат превращается в правдоподобную ошибку. Обосновывать, что вывод ИИ вероятностен и требует проверки, и

[1] Не предполагается использования электронных (цифровых) образовательных ресурсов, являющихся учебно-методическими материалами (мультимедийные программы, электронные учебники и задачники, электронные библиотеки, виртуальные лаборатории, игровые программы, коллекции цифровых образовательных ресурсов), поименованных в федеральном перечне электронных образовательных ресурсов (Приказ Минпросвещения России от 25.08.2026 N 591 «Об утверждении федерального перечня электронных образовательных ресурсов, допущенных к использованию при реализации имеющих государственную аккредитацию образовательных программ начального общего, основного общего, среднего общего образования»)

					закреплять правило «совет дает ИИ, а решает человек».
2.	ИИ + ИБ	Эволюция искусственного интеллекта: от символического ИИ к большим языковым моделям	1	Символический ИИ и экспертные системы, статистическое машинное обучение, глубокое обучение нейронных сетей, трансформеры и большие языковые модели, автономные ИИ-агенты. Движущие факторы развития ИИ. Чем автономнее система, тем выше цена ее ошибки: необходимость верифицируемости, прозрачности и защиты обрабатываемой информации. Перспективы развития отечественной микроэлектроники и центров обработки данных.	Восстанавливать эволюцию ИИ: символьный подход и экспертные системы, статистическое машинное обучение, глубокие нейронные сети, трансформеры и большие языковые модели, автономные агенты. Анализировать движущие факторы развития ИИ: рост объемов данных, доступных вычислений и качества алгоритмов. Объяснять зависимость: чем автономнее система, тем выше цена ее ошибки, и потому нужны верифицируемость, прозрачность и защита данных. Оценивать верифицируемость и объяснимость как условия доверия к автономным ИИ-решениям.
3.	ИИ	Отечественная научная школа и развитие искусственного интеллекта	1	Вклад отечественных ученых в становление 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. Современные достижения российской	Характеризовать вклад отечественных ученых в становление ИИ. Анализировать исторический и этический контекст дискуссии о кибернетике в СССР. Извлекать из этой дискуссии уроки отношения общества к новым

				науки и техники в области ИИ, уникальные условия России для ее технологического лидерства. Исторический и этический контекст: дискуссия о кибернетике в СССР и уроки отношения общества к новым технологиям. Роль отечественных разработок в обеспечении технологического суверенитета. Важность создания собственных вычислительных мощностей, инструментов и наборов данных для обучения моделей ИИ в условиях внешних ограничений.	технологиям и переносить их на современное обсуждение ИИ.
4.	ИИ	Основы нейронных сетей: от модели нейрона к большой языковой модели	1	Формальный нейрон. Идея обучения нейросетей. Почему обучение на данных не равно пониманию: обобщающая способность, переобучение, роль объема и качества обучающей выборки. Статистические методы в основе генерации текста.	Описывать принцип работы формального нейрона и логику обучения нейронной сети на данных. Объяснять, почему обучение на данных не равно пониманию: обобщающая способность, переобучение, роль объема и качества обучающей выборки. Характеризовать статистическую природу генерации текста и связывать ее со способностью модели правдоподобно ошибаться.

					Моделировать на простых примерах, как изменение обучающей выборки влияет на качество предсказаний.
5.	ИБ	Экспертиза информации в эпоху генеративного ИИ	1	Алгоритм оценки источника: первичные и вторичные данные, библиографическая и фактологическая проверка, работа с метаданными и обратным поиском изображений. Когнитивные искажения и манипулятивные техники в подаче информации. Ответственность за репост и производство контента. Специфические ошибки генеративных алгоритмов в составе больших языковых моделей: «галлюцинации», правдоподобная недостоверность; практика верификации ответов ИИ по независимым источникам.	Применять алгоритм оценки источника: различать первичные и вторичные данные, выполнять библиографическую и фактологическую проверку. Работать с метаданными и обратным поиском изображений для подтверждения подлинности информации. Выявлять когнитивные искажения и манипулятивные техники в подаче и объяснять природу «галлюцинаций» генеративного ИИ. Верифицировать утверждения по независимым источникам и демонстрировать ответственность за репост и создание контента.
6.	ИИ	Образ искусственного разума в культуре: от прогноза к инженерной реальности	1	Эволюция представлений об ИИ в литературе, кино и искусстве и их влияние на общественные ожидания и на сами исследования. Разграничение научной фантастики, футурологического прогноза и реальной технологической траектории. Почему ожидания регулярно расходятся с реальностью.	Анализировать эволюцию представлений об ИИ в литературе, кино и искусстве и их влияние на общественные ожидания и сами исследования. Разграничивать научную фантастику, футурологический прогноз и реальную

				Реальные, а не сюжетные риски ИИ: концентрация данных и вычислительных ресурсов, манипуляция, утрата контроля над автономными системами.	технологическую траекторию, объяснять причины их расхождения. Характеризовать реальные, а не сюжетные риски ИИ: концентрацию данных и вычислений, манипуляцию, риск утраты контроля. Аргументированно соотносить культурный образ «думающей машины» с инженерной реальностью современных систем.
7.	ИИ	Этика и право в сфере искусственного интеллекта	1	Ключевые этические проблемы: предвзятость алгоритмов и справедливость, прозрачность и объяснимость, ответственность за решение, приватность. Права человека в цифровой среде: право на объяснение автоматизированного решения, защита от дискриминации, значимые решения – только при участии человека.	Характеризовать ключевые этические проблемы ИИ: предвзятость алгоритмов, справедливость, прозрачность, объяснимость, ответственность за решение, приватность. Объяснять права человека в цифровой среде: право на объяснение автоматизированного решения и защиту от дискриминации. Обосновывать требование участия человека в значимых решениях, принимаемых с помощью ИИ. Оценивать этическую сторону конкретных случаев применения ИИ с опорой на изученные принципы.

8.	ИБ	Социальная инженерия и принцип нулевого доверия: противодействием атаке	1	Атака через доверие: разведка цели, подготовка легенды, канал воздействия, момент действия. Почему человек – «слабое звено» защиты. Вовлечение подростков в уголовно наказуемую деятельность: дропперство, «работа курьером», передача/приём денег, ложные сообщения о минировании по заданию «куратора», вербовка в мессенджерах и онлайн-играх. ИИ как инструмент атакующего: клонирование голоса и лица, генерация убедительных текстов и автоматизация целевого фишинга. Регламенты подтверждения операций, правило «нулевого доверия» к просьбам о данных и деньгах, культура сообщения об инцидентах. Правовые последствия действий подростков в сети с позиции уголовной ответственности: статья 159 УК РФ (мошенничество) и статья 159.6 УК РФ (мошенничество в сфере компьютерной информации), предусматривающие ответственность за хищение путём обмана или доверия, в том числе через воздействие на компьютерную информацию, с максимальным наказанием до десяти лет	Разбирать структуру атаки через доверие: разведку цели, подготовку легенды, канал воздействия и момент действия. Объяснять, почему человек – слабое звено защиты, и формулировать правило нулевого доверия к запросам данных. Характеризовать использование ИИ атакующим: клонирование голоса и лица, генерацию убедительных текстов, автоматизацию целевого фишинга.

				лишения свободы, статья 272 УК РФ – неправомерный доступ к охраняемой компьютерной информации.	
9.	ИИ	Сервисы на основе ИИ: устройство, экономика данных и приватность	1	Как устроены рекомендательные и поисковые сервисы, переводчики, голосовые ассистенты. Экономика данных: «бесплатный» сервис, монетизация поведенческих данных, клиент-серверная архитектура. Управление приватностью: разрешения приложений, настройки рекламных профилей, минимизация оставляемых данных.	Описывать устройство рекомендательных и поисковых сервисов, переводчиков и голосовых ассистентов. Объяснять экономику данных: как бесплатный сервис монетизирует поведенческие данные и почему клиент-серверная архитектура собирает о пользователе больше, чем кажется. Управлять приватностью: настраивать разрешения приложений и рекламные профили, минимизировать оставляемые данные. Оценивать компромисс между удобством сервиса и сохранностью персональных данных.
10.	ИБ	Аутентификация и защита доступа: от пароля к многофакторным схемам	1	Криптографические основы пароля: пространство ключей и трудоемкость перебора, почему важна стойкость и уникальность. Многофакторная и адаптивная аутентификация: одноразовые коды, аппаратные ключи, биометрия и PUSH-подтверждения, менеджер паролей. Настройка	Объяснять криптографические основы пароля: пространство ключей, трудоемкость перебора, важность стойкости и уникальности. Характеризовать многофакторную и адаптивную аутентификацию: одноразовые коды, аппаратные ключи,

				двухфакторной аутентификации на учебном аккаунте, проверка стойкости паролей через открытые сервисы оценки сложности, примеры утечки паролей. Атаки нового типа: подбор по базам утечек, генеративный фишинг и клонирование голоса. Противодействие на уровне человека и устройств.	биометрию, PUSH-подтверждения и менеджер паролей. Выявлять атаки нового типа: подбор по базам утечек, генеративный фишинг и обман систем биометрии.
11.	ИБ	Коммуникации в цифровой среде: этикет, анонимность, доверие и травля	1	Сетевой этикет и правовые рамки общения. Анонимность, верификация личности собеседника и проблема доверия в открытых каналах. ИИ-собеседники: чат-боты и ИИ-агенты в переписке и играх. Кибербуллинг: психология, правовые последствия, алгоритмы безопасного поведения и поддержки пострадавших. Действия при травле в сети. Признаки вовлечения в деструктивные сообщества, алгоритм действий при получении угроз или призывов, координаты горячих линий. Правовые последствия действий подростков в сети с позиции уголовной ответственности: статья 137 УК РФ (нарушение неприкосновенности частной жизни) и статья 137.1 (распространение персональных данных), а также статьи	Соблюдать сетевой этикет и правовые рамки общения в цифровой среде. Анализировать проблемы анонимности, верификации личности собеседника и доверия в открытых каналах. Отличать ИИ-собеседника (чат-бота, ИИ-агента) от человека и объяснять, зачем это нужно с точки зрения безопасности. Распознавать кибербуллинг и деструктивные сообщества и демонстрировать безопасную стратегию реагирования.

				110, 110.1 и 110.2 – доведение до самоубийства, склонение к нему и организация деятельности, побуждающей к нему, статья 128.1 (клевета) применима к распространению заведомо ложных сведений в сети.	
12.	ИИ	Компьютерное восприятие: распознавание изображений, речи и текста	1	Как компьютер «видит» датчиками: 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.	Описывать дискретное представление изображений и звука: пиксель и цветовую модель, звуковой сигнал. Характеризовать распознавание речи и синтез голоса, оптическое распознавание текста, компьютерное зрение и генерацию изображений по описанию. Объяснять трудности распознавания (двусмысленность, иронию, шум в данных) и связанные с ними ошибки моделей. Оценивать риски слежки и неправомерного использования биометрии при массовом компьютерном восприятии.
13.	ИБ	Персональные данные, цифровой след и правовые основы их защиты	1	Правовое содержание понятия персональных данных: категории, основания и цели обработки, права субъекта и обязанности оператора. Цифровой след и профиль: cookie и метаданные, геолокация, поведенческие	Раскрывать правовое содержание персональных данных: категории, основания и цели обработки, права субъекта и обязанности оператора. Описывать цифровой след и профиль (cookie, метаданные, геолокацию,

				данные. Как ИИ собирает разрозненные сигналы в узнаваемый профиль. Цифровая репутация и самопрезентация в сети. Управление приватностью, удаление и переносимость данных. Правовые последствия действий подростков в сети с позиции уголовной ответственности: статья 272.1 УК РФ – незаконные использование, сбор и хранение компьютерной информации, содержащей персональные данные, с усиленной ответственностью при работе с данными несовершеннолетних и биометрией.	поведенческие данные) и объяснять, как ИИ собирает разрозненные сигналы в узнаваемый профиль. Анализировать влияние цифрового следа на репутацию и приватность человека. Формировать осознанное отношение к собственным персональным данным и практике их защиты.
14.	ИБ	Согласия, настройки приватности и профилирование: как устроен сбор данных	1	Правовой смысл согласий и политик конфиденциальности, cookie-уведомления. Что искать в тексте и какие права он ограничивает. Разрешения приложений, профилирование рекламы. Манипулятивные интерфейсы, побуждающие к опасным действиям. Практика настройки приватности в типовых сервисах. Настройки приватности: аудит разрешений установленных приложений на смартфоне с отзывом избыточных разрешений на камеру, микрофон, геолокацию и контакты, настройку	Разбирать правовой смысл согласий и политик конфиденциальности, cookie-уведомлений: что искать в тексте и какие права он ограничивает. Анализировать разрешения приложений и механизмы рекламного профилирования. Выявлять манипулятивные интерфейсы, побуждающие к опасным действиям. Настраивать приватность в типовых сервисах и обосновывать принятые решения.

				cookie в браузере; чтение типового пользовательского соглашения с поиском ключевых пунктов о передаче данных третьим лицам, праве на удаление и юрисдикции.	
15.	ИИ + ИБ	Интернет вещей в умном городе: автоматизация, обратная связь и большие данные	1	Архитектура умного города: сеть датчиков и исполнителей, контур управления с обратной связью. Большие данные и анализ в интересах города: транспорт, ЖКХ, безопасность. Где проходит граница между эффективностью и приватностью при массовом сборе данных. Специфика защищенности: слабые пароли по умолчанию, безопасность беспроводных каналов.	Описывать архитектуру умного города: сеть датчиков и исполнителей, контур управления с обратной связью. Характеризовать применение больших данных в интересах города (транспорт, ЖКХ, безопасность) и проводить границу между эффективностью и приватностью при массовом сборе данных. Объяснять специфику защищенности интернета вещей: слабые пароли по умолчанию и уязвимости беспроводных каналов. Оценивать риски и преимущества умного города с позиций личной и общественной безопасности.
16.	ИИ	Цифровые двойники и компьютерное моделирование	1	От информационных и имитационных моделей к цифровому двойнику. Роль ИИ в двойниках: калибровка параметров, обучение на данных, прогноз состояний и сценарное тестирование без риска для реального объекта. Риски и ответственность:	Различать информационную и имитационную модель и цифровой двойник, объяснять путь от модели к двойнику. Характеризовать роль ИИ в двойниках: калибровку параметров, обучение на данных, прогноз состояний и

				чувствительность данных двойника, последствия неточной модели, вопрос доверия к решениям, принятым на основе модели.	сценарное тестирование без риска для реального объекта. Анализировать риски и ответственность: чувствительность данных двойника, последствия неточной модели, вопрос доверия решению на основе модели. Моделировать простой сценарий с имитационной моделью и обсуждать границы доверия ее выводам.
17.	ИИ + ИБ	Синтетические медиа: дипфейки и технологии противодействия	1	Технологии генерации синтетического контента: архитектуры и обучение, массовость и удешевление подделок аудио, видео и изображений. Методы выявления подделок: анализ артефактов и физиологических сигналов, метаданные и цифровые водяные знаки. ИИ на двух сторонах противостояния. Гигиена достоверности: верификация источника и перепроверка по независимому каналу.	Описывать технологии генерации синтетического контента и объяснять причины массовости и удешевления подделок аудио, видео и изображений. Применять методы выявления подделок: анализ артефактов и физиологических сигналов, работу с метаданными и цифровыми водяными знаками. Характеризовать ИИ на двух сторонах противостояния как инструмент подделки и как средство защиты. Демонстрировать гигиену достоверности: проверку подозрительного медиаконтента по нескольким независимым признакам.
18.	ИБ	Онлайн-мошенничество:	1	Классификация мошеннических схем: фишинг и клонирование сайтов,	Классифицировать схемы онлайн-мошенничества: фишинг и

		схемы, механизмы и порядок действий при инциденте		финансовое и игровое мошенничество. Психологические рычаги воздействия. ИИ как усилитель мошенничества: качество языка, персонализация, имитация голоса и видео, автоматизация массовых и точечных атак. Клонирование голоса из открытых источников. «Голосовое подтверждение» как этап сбора биометрии. Дипфейк-видеозвонок от «значимого взрослого». Фейковое видео с участием известных личностей. Регламент реагирования: фиксация доказательств, блокировка и смена учетных данных, уведомление банка, поддержки сервиса и правоохранительных органов. 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, какие сервисы самозащиты доступны на портале Госуслуг (проверка подозрительного номера, самозапрет на кредиты, проверка кредитной истории).	клонирование сайтов, финансовое и игровое мошенничество, и выявлять их психологические рычаги. Объяснять роль ИИ как усилителя мошенничества: качество языка, персонализацию, имитацию голоса и видео, автоматизацию массовых и точечных атак. Отрабатывать регламент реагирования на инцидент: фиксацию доказательств, блокировку, смену данных, обращение в банк и в полицию. Оценивать надежность предложений и запросов в сети и аргументированно отказывать подозрительным.

				Возможные последствия личного участия в мошенничестве (статья 159 УК РФ).	
19.	ИИ	ИИ в учебной деятельности: инструменты и честность	1	ИИ-инструменты в учебе и труде: объяснение и систематизация материала, генерация задач и тестов, редактура, границы допустимого. Последовательность выполнения учебных заданий: самостоятельное выполнение без обращения к помощи генеративного ИИ; дополнение полученного результата с помощью возможностей ИИ; обобщение и проверка полученных результатов. Академическая честность: ответственность автора, риск делегирования мышления технологиям ИИ.	Применять ИИ-инструменты в учебе для объяснения и систематизации материала, генерации задач и редактуры, соблюдая границы допустимого. Формулировать эффективный запрос, критически оценивать полученный вывод и выполнять проверку фактов и кода. Корректно атрибутировать источники и результат, полученный с помощью ИИ. Обосновывать принципы академической честности и ответственности за учебный результат, созданный при участии ИИ.
20.	ИИ	Генеративный ИИ и интеллектуальное право: вопрос авторства	1	Правовые режимы сгенерированного контента: объект и субъект авторского права, права на изображение и голос, лицензионные условия сервисов, маркировка ИИ-контента. Экономическая и этическая сторона: обучение моделей на чужом творчестве, справедливая компенсация авторов, ответственность за нарушение прав.	Объяснять роль выбора человека как основы авторства сгенерированного произведения. Характеризовать правовые режимы сгенерированного контента: объект и субъект авторского права, права на изображение и голос, лицензионные условия сервисов, маркировку ИИ-контента.

				Правовые последствия действий подростков в сети с позиции уголовной ответственности: нарушение авторских и смежных прав (ст. 146 УК РФ).	Анализировать экономическую и этическую сторону обучения моделей на чужом творчестве и вопрос справедливой компенсации авторам. Аргументированно оценивать правомерность собственных действий с ИИ-контентом.
21.	ИИ	ИИ в медицине: диагностика, метрики качества и ответственность	1	Компьютерное распознавание медицинских изображений и сигналов: задачи, данные, архитектуры. ИИ как «второе мнение» врача. Цена ложноположительного и ложноотрицательного диагноза. Ответственность и этика: врач всегда сам принимает решение. Как датчики и алгоритмы фитнес-устройства получают и интерпретируют показатели. Почему ИИ-совет не заменяет диагностику: риск гипердиагностики и самолечения. Безопасность медицинских данных здоровья: передача и хранение, доступ третьих сторон.	Описывать задачи компьютерного распознавания медицинских изображений и сигналов и роль ИИ как «второго мнения» врача. Объяснять цену ложноположительного и ложноотрицательного диагноза и важность метрик качества модели. Обосновывать, что окончательное решение всегда принимает врач, и оценивать этические последствия автоматизации медицины. Характеризовать особую чувствительность медицинских данных и требования к их защите.
22.	ИИ + ИБ	Безопасность финансовых средств в цифровой среде: архитектура защиты и роль ИИ	1	Архитектура защиты безналичных платежей: клиент-серверная модель и разделение зон ответственности, шифрование канала, протоколы подтверждения, многофакторная	Описывать архитектуру защиты безналичных платежей: клиент-серверную модель и разделение зон ответственности, шифрование канала, протоколы подтверждения,

				аутентификация при проведении операций. Биометрия в финансовом доступе, включая голосовую и поведенческую: требования к защищённости образцов биометрических данных (152-ФЗ) и правовые рамки дистанционного банковского обслуживания (161-ФЗ). Атаки на финансовый доступ: целевой фишинг, клонирование голоса знакомого. Порядок действий и фиксации инцидента, ответственность сторон при компрометации.	многофакторную аутентификацию при операциях. Характеризовать биометрию в финансовом доступе (голосовую, поведенческую) и раскрывать требования к защищённости её образцов (152-ФЗ) и правовые рамки дистанционного банковского обслуживания (161-ФЗ). Разбирать атаки на финансовый доступ (целевой фишинг, клонирование голоса знакомого) и применять регламент реагирования: «пауза перед действием», фиксация доказательств, блокировка и уведомление банка. Оценивать границы доверия ИИ в финансовых операциях, соблюдая принцип курса: подтверждение перевода и ответственность за него остаются за человеком.
23.	ИБ	Вредоносное программное обеспечение и системы защиты	1	Семейства и тактики вредоносного ПО: вирусы, черви, трояны, шпионское и рекламное ПО. Защита: антивирус, межсетевой экран, контроль приложений, обновления, резервное копирование. ИИ в атаке и обороне. Безопасность загрузки и установки программ.	Классифицировать семейства и тактики вредоносного ПО: вирусы, черви, трояны, шпионское и рекламное ПО. Характеризовать средства защиты (антивирус, межсетевой экран, контроль приложений, обновления,

				Проверка устройства антивирусом, настройка межсетевого экрана операционной системы, проверка статуса обновлений операционной системы и браузера, анализ примеров фишинговых писем с поиском признаков подделки – адреса отправителя, ссылок, вложений, срочности просьбы. Правовые последствия действий подростков в сети с позиции уголовной ответственности: статья 273 УК РФ – создание, использование и распространение вредоносных программ.	резервное копирование) и настраивать их. Объяснять применение ИИ в атаке и в обороне. Демонстрировать безопасную практику загрузки и установки программ.
24.	ИИ	Искусственный интеллект в промышленности и сельском хозяйстве: автоматизация и безопасность	1	Промышленный ИИ: компьютерное зрение, предиктивное обслуживание, робототехника и автономные системы (БПЛА, наземные платформы). Понятие периферийного ИИ для работы в условиях отсутствия связи. Защита критической информационной инфраструктуры от кибератак и «отравления данных». Человек в условиях автоматизации: изменение содержания труда, переквалификация, сохранение ответственности человека за критические решения.	Описывать применение промышленного ИИ: компьютерное зрение контроля качества, предиктивное обслуживание оборудования, оптимизацию процессов, робототехнику и беспилотный транспорт в сельском хозяйстве. Анализировать изменение содержания труда в условиях автоматизации и потребность в переквалификации. Обосновывать необходимость сохранения ответственности человека

					за критические решения на автоматизированном производстве. Оценивать перспективы и риски автоматизации для конкретных отраслей.
25.	ИИ + ИБ	ИИ в авиации, космосе и беспилотных системах. Защита каналов связи	1	Автономные и пилотируемые системы: где заканчивается «автопилот» и начинается ИИ. Предиктивное обслуживание техники по данным бортовых датчиков, компьютерное зрение для навигации и уклонения от препятствий, планирование миссий и анализ телеметрии и снимков, помощь диспетчеру и пилоту как «второе мнение». Почему в критических системах решение и ответственность остаются за человеком, а ИИ работает в контуре с обязательной верификацией. Канал связи как часть системы управления и как мишень: связь «Земля – борт – Земля», спутниковая и радионавигация, телеметрия и команды управления беспилотником. Регуляторные требования к кибербезопасности критической инфраструктуры и авиационных систем; этические и правовые вопросы применения беспилотников.	Характеризовать применение ИИ в освоении космоса: автономную навигацию и уклонение марсоходов от препятствий, планирование миссий, анализ сигналов и изображений. Описывать каналы космической связи «Земля – борт – Земля» и их особенности. Выявлять угрозы и меры защиты: помехи и перехват, подмену команд и телеметрии, компрометацию наземного сегмента, криптографию и верификацию. Объяснять, почему задержка сигнала требует автономности, и как совместить ее с безопасностью.

26.	ИИ + ИБ	Профессии на стыке ИИ и информационной безопасности: требования и траектории	1	Профессии в индустрии ИИ и анализа данных: исследователь машинного обучения, инженер данных, аналитик, промпт-инженер, специалист по этике и качеству моделей, инженер по кибербезопасности промышленных систем, разработчик бортовых систем ИИ, специалист по цифровым двойникам, инженер-материаловед с компетенциями в науках о данных (Data Science). Акцент на междисциплинарность: важность физики, химии и математики наравне с программированием. Профессии в информационной безопасности: аналитик, инженер по защите информации, специалист по реагированию на инциденты. Траектория «входа» в профессию: профильное обучение и ЕГЭ, олимпиады, ИТ-специальности вузов и колледжей, портфолио проектов и соревнования. Дефицит и перспективы кадров. «Нецифровые» профессии: расширение возможностей профессиональной деятельности учителя, врача, военного, спасателя и т.д. навыками в сфере ИИ	Характеризовать роли в индустрии ИИ и данных: исследователь машинного обучения, инженер данных, аналитик, промпт-инженер, специалист по этике и качеству моделей. Описывать роли в информационной безопасности: аналитик, инженер по защите информации, специалист по реагированию на инциденты. Планировать траекторию «входа» в профессию: профильное обучение и ЕГЭ, олимпиады, вузы и колледжи, портфолио. Соотносить личные интересы и способности с требованиями профессий на стыке ИИ и информационной безопасности.

				для стабилизации социально-экономической ситуации на рынке труда.	
27.	ИИ + ИБ	Личная стратегия работы с ИИ и информационной безопасности: итоговая рефлексия	1	Формирование персональной методики: с какими ИИ-сервисами работаю, для каких задач, как проверяю результат и что не доверяю модели. Формируем личную позицию «ИИ – это…», «он умеет…», «в нем нельзя…», «как я себя берегу». Закрепление главного принципа: совет дает ИИ, решает человек. План развития компетенций ИИ и ИБ после окончания школы.	Формировать персональную методику работы с ИИ: с какими сервисами и для каких задач работать, как проверять результат и что не доверять модели. Аргументированно выражать личную позицию: «ИИ – это…», «он умеет…», «в нем нельзя…», «как я себя берегу». Закреплять главный принцип безопасной работы: совет дает ИИ, решает человек.
Итого:			27		



Федеральное государственное бюджетное научное учреждение
«Институт содержания и методов обучения им. В.С. Леднева»

Рабочая программа курса внеурочной деятельности

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

(основное общее образование)

Москва
2026

СОДЕРЖАНИЕ

Пояснительная записка 3
Содержание курса внеурочной деятельности 7
5-7 классы 7
8-9 классы 13
Планируемые результаты освоения программы курса внеурочной деятельности 20
Личностные результаты 20
Метапредметные результаты 23
Предметные результаты 27
Тематическое планирование 32
5-7 классы 32
8-9 классы 45

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.

Тематическое планирование

5-7 классы

№ / акцент занятия		Наименование тем курса[1]	Кол-во часов	Программное содержание	Характеристика деятельности обучающихся
1.	ИИ + ИБ	Искусственный интеллект и как с ним общаться безопасно	1	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.	Рассказывать, что такое искусственный интеллект и какие задачи он решает. Сопоставлять возможности компьютера и человеческого интеллекта; характеризовать сходство и различия роботов и ИИ. Различать достоверную и недостоверную информацию об ИИ, отделять мифы от реальных возможностей технологий. Формулировать главное правило безопасного общения с ИИ: «совет дает ИИ, а решает человек».

[1] Не предполагается использования электронных (цифровых) образовательных ресурсов, являющихся учебно-методическими материалами (мультимедийные программы, электронные учебники и задачники, электронные библиотеки, виртуальные лаборатории, игровые программы, коллекции цифровых образовательных ресурсов), поименованных в федеральном перечне электронных образовательных ресурсов (Приказ Минпросвещения России от 25.08.2026 N 591 «Об утверждении федерального перечня электронных образовательных ресурсов, допущенных к использованию при реализации имеющих государственную аккредитацию образовательных программ начального общего, основного общего, среднего общего образования»)

2.	ИИ + ИБ	Эволюция нейросетей и информационная безопасность	1	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.	Характеризовать исследования ученых в области разработки ИИ и основные этапы пути от первых программ к ИИ-агентам. Анализировать возможности и сферу применения ИИ на разных этапах его развития. Объяснять, почему с ростом «умности» компьтера важны навыки безопасного обращения с данными.
3.	ИИ	Вклад российских ученых в развитие искусственного интеллекта	1	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.	Характеризовать вклад отечественных ученых в развитие ИИ и примеры помощи ИИ науке. Приводить примеры использования ИИ в научных исследованиях: перебор вариантов, поиск закономерностей в больших данных.
4.	ИИ	Как мы думаем и как «думает» компьютер: про нейроны и	1	Думать, запоминать и решать задачи помогает головной мозг: он собирает ощущения, сравнивает с прошлым опытом и выбирает действие. Головной мозг и	Характеризовать особенности функционирования мозга при получении и передаче информации; раскрывать смысл понятия

		нейросети		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.	«нейрон». Находить сходство и отличия мышления человека и работы компьютера. Объяснять принцип работы нейросети на уровне аналогии и ее отличия от живого мышления. Моделировать работу нейронной сети на доступном примере.
5.	ИБ	Правда или выдумка: учимся проверять информацию	1	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.	Различать факт и мнение; выявлять признаки ложной и подозрительной публикации. Сравнивать источник с другим, проверять информацию по нескольким независимым источникам. Оценивать ответы ИИ как источник, требующий обязательной проверки. Участвовать в обсуждении, аргументировать собственную точку зрения и приводить контраргументы.
6.	ИИ	Фантастика в прошлом – реальность в настоящем	1	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» –	Соотносить образ «думающей машины» в литературе, кино и живописи с современными технологиями. Различать достоверную и

				это не настоящая опасность, а использование ИИ в реальности влечет угрозы, которые нужно уметь узнавать.	недостоверную информацию об ИИ, узнавать популярные мифы. Объяснять, почему вымышленная опасность робота отличается от реальных рисков использования ИИ.
7.	ИИ	Этика и мораль для искусственного интеллекта	1	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.	Раскрывать смысл и содержание этики и морали ИИ; перечислять принципы, которым компьютер учат люди. Характеризовать право и защиту человека от злоупотреблений ИИ. Осознавать важность правила «решает человек» и приводить примеры его применения.
8.	ИБ	Обманывать в сети тоже плохо. Обман на доверии	1	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	Характеризовать приемы обмана в сети: торопят, пугают, льстят, чтобы выманить данные и пароли. Выявлять признаки манипуляции в переписке и по телефону на понятных примерах. Объяснять, как ИИ делает обман

				интернете, сообщить родителям или педагогу, сохранить переписку. ИИ делает обман убедительным, ведь голос и лицо «близкого» человека можно подделать.	убедительным через подделку голоса и лица.
9.	ИИ	ИИ вокруг нас каждый день: телефон, навигатор, умная колонка	1	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.	Анализировать возможности и сферу применения ИИ в повседневной жизни. Приводить примеры ИИ-помощников в телефоне, навигаторе, умной колонке, играх. Объяснять, какие данные собирают помощники о пользователе.
10.	ИБ	Пароль как ключ от двери: делаем его надежным	1	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.	Раскрывать смысл понятия «пароль» и объяснять его роль как ключа от цифровой комнаты. Составлять надежные пароли и соблюдать правила их уникальности и неразглашения. Характеризовать назначение менеджера паролей и двухфакторную проверки. Объяснять, почему ИИ угадывает простые пароли, и беречь учетные данные.

11.	ИБ	Общаемся в сети безопасно: мессенджеры и незнакомцы	1	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.	Понимать, что по содержанию переписки нельзя надежно установить личность и природу собеседника. Применять правила проверки и безопасного общения независимо от убедительности сообщения. Знать и соблюдать правила безопасного общения в мессенджерах и игровых чатах. Различать, кто по другую сторону экрана - человек или ИИ; распознавать опасные знакомства. Характеризовать признаки просьбы о личных данных и уметь отказывать. Участвовать в обсуждении сетевого этикета, формулировать правила поведения в группе.
12.	ИИ	Как ИИ «видит», «слышит», «говорит»	1	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.	Сравнивать особенности зрения, слуха и речи человека и компьютера. Характеризовать распознавание образов, речи и текста; перечислять сферы применения. Объяснять, почему компьютеру трудно распознать шутку и двусмысленность.

13.	ИБ	Мои данные и цифровой след: все сохраняется надолго	1	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.	Раскрывать смысл понятия «персональные данные» и «цифровой след». Объяснять, почему все, попавшее в сеть, сохраняется надолго и влияет на репутацию. Характеризовать ответственную публикацию и цифровую репутацию. Анализировать собственные цифровые следы и делать выводы о защите данных.
14.	ИБ	Кто собирает мои данные: настройки и согласия сайтов	1	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.	Объяснять, как сайты и приложения собирают данные и зачем это. Настраивать приватность и разрешения, управлять геолокацией. Читать простые правила согласия и находить в них существенные пункты. Объяснять, как собранные данные питают ИИ-рекомендации и влияют на показываемый контент.
15.	ИИ + ИБ	«Умный» дом и «умный» город: как техника заботится о нас	1	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	Характеризовать возможности применения ИИ в умном доме и умном городе. Описывать контур «датчик - решение - исполнитель» на примере умного дома. Объяснять, как в собирающем

				безопасный город, распознавание номеров). Как в городе, который все измеряет и собирает данные о людях, стирается граница приватности.	данные городе стирается граница приватности.
16.	ИИ	Цифровые двойники: точная копия для опытов без вреда	1	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.	Раскрывать смысл понятия «цифровой двойник». Называть плюсы и минусы цифровой копии для опытов без вреда для оригинала. Объяснять, как ИИ обучается и предсказывает на модели двойника.
17.	ИИ + ИБ	Подделка и обман: как ИИ создает фейки и как их узнать	1	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.	Объяснять, как ИИ создает синтетические подделки: видео, записи голоса, сообщения. Выявлять признаки подделки; различать, кто это сделал и откуда это. Характеризовать роль ИИ и для мошенников, и для защитников. Соблюдать правило не сообщать код из СМС; применять регламент проверки источника.
18.	ИБ	Ловушки в сети: как распознать мошенника	1	Приманка всегда выглядит заманчиво или страшно, ее цель вывести из безопасного интернет-пространства. Подозрительные письма и ссылки (письма-приманки),	Выявлять признаки приманки: подозрительные письма и ссылки, фальшивые подарки и «легкие деньги».

				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).	Объяснять, как ИИ делает приманки убедительнее, и применять правила проверки. Характеризовать алгоритм действий, если обман совершен.
19.	ИИ	Учусь честно: нейросеть мне помогает, а не делает работу за меня	1	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.	Демонстрировать усвоение последовательности действий: самостоятельная попытка решения; фиксация возникшего затруднения; разрешенное педагогом обращение к ограниченной подсказке; проверка ответа; самостоятельное объяснение итогового решения. Демонстрировать навыки работы с ИИ при изучении «трудных вопросов» по учебному предмету. Формулировать запрос, чтобы нейросеть объяснила непонятное и составила вопросы для самопроверки.

					Соблюдать правила честности: сначала подумай сам, потом сверься; не выдавай сгенерированное ИИ за свое. Давать оценку результатам работы с ИИ и анализировать ее.
20.	ИИ	ИИ рисует и сочиняет: кто здесь автор	1	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.	Различать сходства и отличия творчества человека и ИИ. Раскрывать вопрос авторства: кто автор сгенерированного произведения. Сравнивать результаты индивидуального творчества и работы ИИ; отмечать сделанное с помощью ИИ.
21.	ИИ	ИИ на страже здоровья: границы доверия	1	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.	Характеризовать возможности применения ИИ при диагностике заболеваний. Сравнивать, что замечает человек и что выявляет компьютер, и почему им лучше работать вместе. Оценивать достоверность информации о здоровье, полученной с помощью ИИ. Объяснять, почему диагноз и забота о пациенте остаются ответственностью врача.
22.	ИИ	Безопасность	1	Онлайн-банкинг и банковские приложения.	Рассказывать, как с помощью

	+ ИБ	финансовых средств в цифровой среде		Системы для защиты платежей и данных клиентов от злоумышленников. Голосовая биометрия. Типовые схемы атак на семейный бюджет.	банковского приложения можно платить и переводить деньги и какие данные для этого нужны. Объяснять как банк защищает платежи и данные клиента от злоумышленников: пароли и подтверждения; проверка операции; напоминание, что банк никогда не спрашивает коды и полные данные карты. Приводить примеры типовых схем обмана семейного бюджета (звонки «из банка», «замороженные» и «ошибочные» переводы, лёгкие деньги) и демонстрировать правило: не сообщать коды и данные карты, положить трубку и перезвонить в банк по номеру с обратной стороны карты.
23.	ИБ	Почему «заболел» компьютер: вредоносные программы	1	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.	Раскрывать смысл понятия «вредоносные программы»; объяснять, почему компьютер может «заболеть». Характеризовать признаки заражения и пути распространения опасных файлов. Соблюдать правила безопасной загрузки и установки программ; объяснять роль антивируса.

					Объяснять, как ИИ помогает и антивирусам, и тем, кто прячет вирусы.
24.	ИИ	ИИ на заводе и в поле: быстрее, больше, лучше	1	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.	Характеризовать возможности применения ИИ в промышленности и сельском хозяйстве. Перечислять виды помощи ИИ: контроль качества, оптимизация, робототехника. Анализировать, какая работа переходит к компьютеру и какая остается за человеком. Приводить примеры реализации возможностей ИИ на производстве.
25.	ИИ + ИБ	Искусственный интеллект и информационная безопасность в космосе	1	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.	Анализировать примеры применения ИИ в космосе: автопилоты, распознавание снимков Земли, поиск сигналов. Объяснять роль ИИ в ускорении научных и инженерных задач. Характеризовать риски и угрозы при передаче данных между Землей и космосом.
26.	ИИ + ИБ	Кем быть: профессии, где нужен искусственный	1	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	Перечислять профессии в сфере ИИ и описывать их функции, включая специалиста по кибербезопасности. Сопоставлять задачи профессии и

		интеллект		профессий – специалист по кибербезопасности.	нужные для нее школьные знания. Характеризовать применение ИИ в бизнесе и повседневной работе. Участвовать в дискуссии, формулировать личную позицию о будущем профессий.
27.	ИИ + ИБ	Я, нейросеть и моя безопасность: итоговый разговор	1	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.	Повторять изученный материал и развивать навыки рефлексии и самоконтроля. Собирать личный «паспорт безопасности» из изученных правил. Формулировать обобщающие суждения: что такое ИИ, что он может, в чем его выводы нельзя принимать без проверки, как себя беречь.
		Итого:	27		

8-9 классы

№ / акцент занятия		Наименование тем курса[2]	Кол-во часов	Программное содержание	Характеристика деятельности обучающихся
1.	ИИ + ИБ	Искусственный интеллект: какие задачи он решает и где ошибается	1	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.	Рассказывать, какие задачи ИИ решает на уровне человека: распознавание образов и речи, генерация текста и изображений, планирование, игра. Объяснять отличие обучаемой модели от обычной программы: ее результат формируется на основе данных, а не задается жесткой инструкцией. Характеризовать границы применимости: почему модель, хорошо решающая одну задачу, беспомощна в другой. Формулировать ключевое правило: совет дает ИИ, а решение и ответственность - за человеком.

[2] Не предполагается использования электронных (цифровых) образовательных ресурсов, являющихся учебно-методическими материалами (мультимедийные программы, электронные учебники и задачники, электронные библиотеки, виртуальные лаборатории, игровые программы, коллекции цифровых образовательных ресурсов), поименованных в федеральном перечне электронных образовательных ресурсов (Приказ Минпросвещения России от 25.08.2026 N 591 «Об утверждении федерального перечня электронных образовательных ресурсов, допущенных к использованию при реализации имеющих государственную аккредитацию образовательных программ начального общего, основного общего, среднего общего образования»)

2.	ИИ + ИБ	Эволюция идей искусственного интеллекта: от логических правил к обучению на данных	1	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.	Описывать основные этапы развития ИИ: от символического ИИ и экспертных систем до генеративных моделей и ИИ-агентов. Анализировать роль накопления данных и роста вычислительных мощностей в этом развитии. Характеризовать новые риски: чем автономнее система, тем важнее контроль человека и защита обрабатываемой информации.
3.	ИИ	Вклад отечественных ученых в развитие искусственного интеллекта	1	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.	Характеризовать вклад отечественных ученых в развитие ИИ и примеры помощи ИИ науке. Приводить примеры использования ИИ в научных исследованиях: перебор вариантов, поиск закономерностей в больших данных, предсказание свойств веществ. Работать с ресурсами сети для сбора сведений о дискуссии по кибернетике и становлении отечественной школы.

4.	ИИ	Как устроена искусственная нейронная сеть: от формального нейрона к обучаемой модели	1	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.	Характеризовать статистический характер вывода: почему сеть с миллионами параметров не понимает текст. Формулировать уточняющие запросы, отличая рассуждение человека от ответа ИИ.
5.	ИБ	Достоверность информации и методы ее проверки: факт, оценка, источник	1	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.	Разграничивать факт, оценку и мнение. Применять критерии достоверности и актуальности источника, перекрестную проверку и работу с первичными публикациями. Выявлять признаки сфабрикованной и манипулятивной информации; проверять метаданные и водяные знаки. Оценивать ответ нейросети как источник, требующий такой же проверки, как и любой внешний.
6.	ИИ	От научной фантастики к инженерии: какими представляли умные машины и что стало технологией	1	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,	Соотносить образ «думающей машины» в литературе и кино с современными технологиями. Объяснять, почему «восставший робот» – сюжетный прием, а не настоящая опасность. Характеризовать реальные риски: слежку, дезинформацию, манипуляцию и утрату контроля.

				дезинформацией, манипуляцией и утратой контроля. Умение узнавать настоящие угрозы.	Демонстрировать навыки различения достоверной и недостоверной информации об ИИ.
7.	ИИ	Этика и правовое регулирование искусственного интеллекта	1	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».	Называть этические принципы ИИ: справедливость, прозрачность, объяснимость, безопасность, подотчетность. Характеризовать права человека в среде ИИ-сервисов: защиту от дискриминации алгоритмами, право на объяснение. Обосновывать принцип «человек принимает решение» и приводить примеры его применения.
8.	ИБ	Социальная инженерия: как обманывают не компьютер, а человека	1	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	Описывать психологические приемы обмана: дефицит времени, страх, лесть, авторитет, жадность. Характеризовать типовые сценарии атак и объяснять, как ИИ усиливает манипуляцию подделкой голоса, лица и текста. Применять личный алгоритм: пауза, проверка по независимому каналу, отказ называть код и персональные данные.

				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.	
9.	ИИ	ИИ в повседневных цифровых сервисах: принципы работы, настройки, приватность	1	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	Анализировать принципы работы привычных сервисов: поисковой выдачи и рекомендаций, перевода, распознавания речи. Объяснять зависимость обучаемой модели от данных пользователя. Называть, какие данные собирают сервисы, и ограничивать это настройками приватности и

				разрешениями приложений.	разрешениями приложений.
10.	ИБ	Аутентификация и защита доступа	1	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.	Объяснять связь между длиной пароля, мощностью используемого алфавита и числом возможных комбинаций. Различать факторы аутентификации: пароль, одноразовый код, биометрию, аппаратный ключ. Обосновывать требования к стойкости и уникальности пароля, назначение двухфакторной защиты и менеджера паролей. Объяснять, как ИИ помогает атакующим: подбор по словарям и базам утечек, подделка голоса знакомого.
11.	ИБ	Безопасное общение в цифровой среде: сетевой этикет, анонимность, верификация собеседника	1	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	Понимать, что по содержанию переписки нельзя надежно установить личность и природу собеседника. Применять правила проверки и безопасного общения независимо от убедительности сообщения. Характеризовать сетевой этикет и способы противодействия кибербуллингу. Верифицировать собеседника,

				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.	помня, что по другую сторону экрана может быть и человек, и ИИ-агент. Выявлять признаки опасных знакомств и уметь отказывать в просьбах о данных и деньгах. Формулировать правила защиты своего устройства и аккаунтов.
12.	ИИ	Компьютерное распознавание изображений, речи и текста: признаки, модели, ошибки	1	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.	Объяснять принцип компьютерного восприятия через дискретное представление данных: пиксель, цветовую модель, частоту дискретизации. Характеризовать задачи распознавания речи, образов и текста и их типичные ошибки. Объяснять трудности распознавания: двусмысленность, иронию, шум в данных. Оценивать риски слежки и называть этические ограничения работы с биометрией.
13.	ИБ	Персональные данные, цифровой след и цифровая	1	Что относится к персональным данным и как они защищаются. Права субъекта данных. Цифровой след: cookie, метаданные переписки, публикации,	Раскрывать, что относится к персональным данным, и называть права субъекта данных. Характеризовать цифровой след:

		репутация		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.	cookie, метаданные переписки, публикации, геолокацию. Объяснять, как ИИ связывает разрозненные данные в профиль и находит человека по косвенным признакам. Управлять цифровой репутацией: решать, что публиковать безопасно, как ограничивать сбор и удалять данные.
14.	ИБ	Согласия, настройки приватности и профилирование: кто и как собирает данные	1	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.	Читать пользовательские соглашения и политики конфиденциальности, находить в них существенные пункты. Настраивать разрешения приложений: геолокацию, микрофон, камеру, контакты. Характеризовать профилирование, персонализацию рекламы. Объяснять, как собранные данные питают ИИ-рекомендации и влияют на показываемый контент.
15.	ИИ + ИБ	Промышленный и бытовой интернет вещей в умном городе: автоматизация, обратная связь,	1	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.	Описывать контур «датчик – сигнал – решение – исполнитель» в умном доме и умном городе. Анализировать пользу больших данных и цифровых платформ города и границу приватности при

		большие данные		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.	тотальном сборе. Характеризовать типовые уязвимости IoT: пароли по умолчанию, уязвимые прошивки, открытые сети.
16.	ИИ	Цифровые двойники	1	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.	Раскрывать смысл понятия «цифровой двойник» как динамической компьютерной модели объекта. Характеризовать роль ИИ в калибровке и прогнозировании двойника. Описывать экспериментирование на двойнике без риска для оригинала. Оценивать риски чувствительности данных двойника и использования копии против оригинала.
17.	ИИ + ИБ	Синтетические медиа: дипфейки и методы их обнаружения	1	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.	Объяснять принцип генерации реалистичных видео, аудио и изображений на основе глубоких моделей. Выявлять признаки подделки: артефакты, несогласованность мимики, метаданные, водяные знаки, отсутствие подтверждения в независимых источниках.

				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».	Характеризовать роль ИИ на обеих сторонах - и на стороне подделки, и на стороне защиты. Применять регламент «не верь глазам - проверь источник, уточни у адресата, не сообщай коды».
18.	ИБ	Онлайн-мошенничество: технические и социальные механизмы, действия после инцидента	1	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	Классифицировать типовые схемы: фишинговые письма и ссылки, фальшивые конкурсы и «легкие деньги», поддельные службы поддержки. Объяснять, как ИИ усиливает приманки: безупречный язык, персонализация, имитация голоса, массовые рассылки. Характеризовать алгоритм действий после инцидента: зафиксировать доказательства, сменить пароли, сообщить взрослым, обратиться в поддержку и полицию.

				УК РФ).	
19.	ИИ	Нейросеть как инструмент обучения, а не замена мышлению: академическая честность	1	Роль ИИ в учебной работе: разобрать сложное, составить вопросы для самопроверки, проверить черновик, стать тренажером формулировок. Риски привычки немедленно обращаться к ИИ при любом затруднении. Приемы формулирования запроса и обязательная проверка результата. 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.	Демонстрировать усвоение последовательности действий: самостоятельная попытка решения; фиксация возникшего затруднения; разрешенное педагогом обращение к ограниченной подсказке; проверка ответа; самостоятельное объяснение итогового решения. Формулировать запрос к генеративной модели для объяснения сложного, самопроверки и проверки черновика. Распознавать ошибки модели и ссылаться на источник и авторство идеи. Соблюдать правила академической честности: сначала решить самому, потом сверяться; не выдавать сгенерированное ИИ и чужое за свое. Анализировать и оценивать полноту и корректность ответа модели.
20.	ИИ	Генеративный ИИ и авторское право: кто автор созданного ИИ произведения	1	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:	Объяснять принцип генерации текста, изображений и музыки: модель - инструмент, а замысел и выбор остаются за человеком. Различать 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.	авторское право, права на изображение и голос, маркировку ИИ-контента. Отмечать работу, выполненную с помощью ИИ, и ответственно относиться к чужому труду.
21.	ИИ	ИИ на службе медицины: задачи диагностики, ограничения, ответственность	1	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.	Характеризовать задачи компьютерного распознавания медицинских изображений и сигналов: снимков, кардиограмм. Объяснять, почему ИИ эффективен как «второй взгляд», но не заменяет врача. Оценивать качество модели через цену ложноположительного и ложноотрицательного решения и проверку на реальных данных. Называть медицинские данные особо чувствительной категорией и обосновывать их защиту.
22.	ИИ + ИБ	Безопасность финансовых средств в цифровой среде	1	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»	Характеризовать системы защиты платежей и данных клиентов в онлайн-банках: зачем нужны коды подтверждения и ограниченные права доступа, почему банк никогда не спрашивает полные данные карты или код из SMS. Объяснять роль биометрии при

				переводы, поддельные операции по карте, мошенничество с рассрочками и микрокредитами.	аутентификации и её уязвимости. Выявлять типичные схемы атак на семейный бюджет: понимать логику работы «замороженных» и «ошибочных» переводов, фальшивых служб поддержки и предложения оформить микрокредит, объясняя, что все эти методы построены на доверии и искусственной срочности.
23.	ИБ	Вредоносное программное обеспечение и современные средства защиты	1	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).	Классифицировать вредоносное ПО: вирусы, черви, трояны, шифровальщики, шпионское ПО. Называть пути распространения и признаки заражения. Объяснять принцип действия антивируса и роль машинного обучения в обнаружении новых образцов. Соблюдать правила безопасной загрузки и обосновывать важность обновлений и резервного копирования.
24.	ИИ	Искусственный интеллект в промышленности и сельском хозяйстве: автоматизация и	1	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	Характеризовать задачи ИИ на производстве: компьтерное зрение для контроля качества, роботизированные линии, умное сельское хозяйство и транспорт. Объяснять, почему «умное»

		безопасность		человеком. Чем «умнее» производство, тем оно уязвимее для информационных атак: защита критической инфраструктуры.	производство уязвимее для информационных атак. Называть меры защиты критической инфраструктуры.
25.	ИИ + ИБ	ИИ в авиации, космосе и беспилотных системах. Защита каналов связи	1	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.	Анализировать примеры применения ИИ в космосе для распознавания снимков, планирования миссий. Описывать канал «Земля – борт – Земля» и последствия значительной задержки сигнала для управления. Характеризовать угрозы передачи данных: перехват, подмену команд и телеметрии, компрометацию наземного сегмента. Называть принципы защиты космических систем связи.
26.	ИИ + ИБ	Профессии на стыке ИИ и информационной безопасности: требования и траектории	1	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	Перечислять профессии цикла данных и ИИ и профессии информационной безопасности, описывать их задачи. Сопоставлять задачи профессии и востребованные школьные знания: программирование, алгоритмизацию, основы сетей и криптографии, работу с большими данными. Характеризовать индивидуальную

				большими данными. Важность физики и инженерного мышления. Индивидуальная траектория: профильные предметы, олимпиады, ОГЭ по информатике, проекты и дополнительные курсы.	траекторию: профильные предметы, олимпиады, ОГЭ по информатике, проекты и курсы. Формулировать личную позицию о будущем профессий и участвовать в дискуссии.
27.	ИИ + ИБ	Личный регламент работы с ИИ и базовые правила информационной безопасности	1	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.	Повторять изученный материал и развивать навыки рефлексии и самоконтроля. Собирать личный «паспорт безопасности» и регламент работы с ИИ-сервисами. Формулировать обобщающие суждения: что такое ИИ, что он может, почему его выводы нельзя принимать без проверки, как себя беречь.
Итого:			27		