**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Министерство просвещения, науки и по делам молодежи Кабардино-Балкарской Республики**

**Местная администрация Терского муниципального района КБР**

**МКОУ СОШ с.п. Верхний Акбаш**

| РАССМОТРЕНА | СОГЛАСОВАНА | УТВЕРЖДЕНА |
|---|---|---|
| Методическим объединением↲учителей математики, физики и↲информатики<br>Тенова Р.Х.<br>Протокол №1 от «27» 08 2026 г. | Зам. директора по УВР<br>_____<br>Гонибова Ж.Ш.<br>. от «27» 08 2026 г. | Директор<br>_____<br>Тарканова М.В.<br>Приказ №87 от «28» 08 2026 г. |

**РАБОЧАЯ ПРОГРАММА**

**курса внеурочной деятельности «Искусственный интеллект и информационная безопасность»**

для обучающихся 8–9 классов

**Верхний Акбаш 2026г.**

# 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»

## 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
## 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
## 8–9 классы

| № / акцент занятия | Наименование тем курса[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 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. 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. |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **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. |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **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, дезинформацией, манипуляцией и утратой контроля. Умение узнавать настоящие угрозы. | 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. Демонстрировать навыки различения достоверной и недостоверной информации об ИИ. |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **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 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. | 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. |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **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 разрешениями приложений. | 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. |
| **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. |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **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 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. | 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, 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. |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **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 репутация | 1 | 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. | Раскрывать, что относится к персональным данным, и называть права субъекта данных. Характеризовать цифровой след: 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. |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **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, большие данные | 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. 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. | Описывать контур «датчик – сигнал – решение – исполнитель» в умном доме и умном городе. Анализировать пользу больших данных и цифровых платформ города и границу приватности при тотальном сборе. Характеризовать типовые уязвимости IoT: пароли по умолчанию, уязвимые прошивки, открытые сети. |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **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. 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». | 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. 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». |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **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 УК РФ). | 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. |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **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. |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **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: 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. | 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, 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. |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **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» переводы, поддельные операции по карте, мошенничество с рассрочками и микрокредитами. | 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 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. |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **24. ИИ** | Искусственный интеллект в промышленности и сельском хозяйстве: автоматизация и безопасность | 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 человеком. Чем «умнее» производство, тем оно уязвимее для информационных атак: защита критической инфраструктуры. | Характеризовать задачи ИИ на производстве: компьтерное зрение для контроля качества, роботизированные линии, умное сельское хозяйство и транспорт. Объяснять, почему «умное» 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. |

| № / акцент занятия | Наименование тем курса[1] | Кол-во часов | Программное содержание | Характеристика деятельности обучающихся |
|---|---|---|---|---|
| **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 большими данными. Важность физики и инженерного мышления. Индивидуальная траектория: профильные предметы, олимпиады, ОГЭ по информатике, проекты и дополнительные курсы. | 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 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** | | |