Кинельское управление Министерства образования Самаркой области
Государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа № 11 г. Кинеля городского округа Кинель Самарской области

Принята на заседании
Педагогического совета Учреждения
от «03» ноября 2026 г.
Протокол № 3

Утверждена:
Приказом №807/1-ОД
от «03» ноября 2026 г.
Директор ГБОУ СОШ №11 г.Кинеля
_____ О.А. Лозовская

ЭП

C=RU, O=ГБОУ СОШ №. 11 г.Кинеля, CN=Лозовская О.А., E=knl_11sch@63edu.ru
00c03129bad29e261f
2026.11.03 18:55:47+04'00'

Дополнительная общеобразовательная общеразвивающая программа

«Искусственный интеллект и информационная безопасность»

техническая направленность

Возраст обучающихся: 15-17 лет
Срок реализации: 1 год

Разработчик:
учитель информатики
Никитина Екатерина Сергеевна

г. Кинель 2026 г.

Оглавление

Аннотация к программе ……..3
Пояснительная записка ……..…….4
Учебно-тематический план……...…….26
Содержание ……48
Воспитательный компонент ……....58
Обеспечение программы…….…..59
Список литературы ……...61
Приложение «Годовой календарный учебный график» ……...……62

Аннотация к программе

Дополнительная общеобразовательная общеразвивающая программа технической направленности «Искусственный интеллект и информационная безопасность» (далее – Программа) рассчитана на 1 год. 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. Совершенствование цифровых навыков обучающихся 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.

Данная программа адаптирована для детей с ОВЗ.

Пояснительная записка

Дополнительная общеобразовательная общеразвивающая программа «Искусственный интеллект и информационная безопасность» направлена на развитие компетенций обучающихся в области современных информационных и коммуникационных технологий (ИКТ), основанных на достижениях науки и IT-отрасли. Содержание программы 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).

Дополнительная общеразвивающая программа «Искусственный интеллект и информационная безопасность» ориентирована на:

− приоритеты и перспективы, обозначенные в Стратегии научнотехнологического 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».

Программа составлена в соответствии с основными нормативно-правовыми документами:

Федеральным Законом «Об образовании» от 29.12.2012 г. № 273-ФЗ;

Порядком организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам от 09.11.2018 г. № 196;

Целевой моделью развития региональных систем дополнительного образования детей от 03.09.2019 г. № 467;

Концепцией развития дополнительного образования детей до 2030 года утвержденной распоряжением Правительства Российской Федерации от 31.03.2022 №678-р;

Санитарно-эпидемиологическими требованиями к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи от 28.09.2020 г. № 28.

Данная ***программа технической направленности*** включает 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 старшеклассников этот блок приобретает дополнительное значение: содержание программы связано с профессиональным самоопределением и показывает траектории входа в профессии на стыке ИИ и информационной безопасности.

Данная программа адаптирована для детей с ОВЗ.

При реализации данной программы будет задействовано оборудование центра «Точка Роста».

Актуальность программы

«Сквозные» технологии цифровой экономики Российской Федерации – это перспективные технологии, радикально меняющие ситуацию на существующих рынках или способствующие формированию новых рынков. Выделяют 9 технологий, среди которых присутствуют технологии искусственного интеллекта (далее - ИИ). Квалифицированные и компетентные кадры являются основой для развития страны и ключевых отраслей производства, позволяя экономике адаптироваться к появлению передовых технологий, связанных с ИИ. Поэтому в современном мире как никогда требуются специалисты в данной области.

Экономика, основанная на ИИ, требует нового подхода к национальной системе образования, включая способы предоставления знаний в области ИИ более широкой аудитории, не имеющей технического образования, социальных и технических навыков для применения ИИ в реальной жизни. Однако, если техническое и социальное понимание ИИ будет ограничено только крупными организациями, технологическими компаниями, научно-исследовательскими институтами и высшими учебными заведениями, то общий уровень знаний и понимания сути ИИ останется низким, поэтому существует острая необходимость в том, чтобы обучать школьников основам ИИ.

Программа предусматривает формирование у учащихся мотивации, устойчивых умений, овладение инструментарием для решения социально значимых задач в реальной жизни.

Задача педагога – развить у обучающихся навыки самостоятельного создания нейронных сетей и использования уже имеющихся, тем самым создав основу для дальнейшего изучения данного направления.

Изучение программы ««Искусственный интеллект и информационная безопасность»» базируется на совокупности теоретических знаний в работе с нейронными сетями и практических навыках создания и интеграции нейронных сетей. Этот подход способствует расширению знаний обучающихся в области

алгоритмизации, стимулирует системное мышление и развивает творческий потенциал, способствуя личностному росту.

Отличительная особенность программы обусловлена перечнем приоритетов и перспектив научно-технологического развития Российской Федерации, перечисленных в Стратегии научно-технологического развития Российской Федерации, где создание систем обработки больших объемов данных, машинного обучения и искусственного интеллекта названо в числе приоритетных направлений научно-технологического развития Российской Федерации на ближайшие 10-15 лет.

Обучение учащихся в сфере искусственного интеллекта и информационной безопасности носит интегративный и практикоориентированный характер; способствует развитию интереса к учебнопознавательной 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.

Педагогическая целесообразность

Образовательная программа ««Искусственный интеллект и информационная безопасность»» обосновывается возможностью оказания долгосрочного воздействия на формирование личности ученика и предоставления обширных шансов для самовыражения через использование искусственного интеллекта на практике. Ее фокус останавливается на инженерно-практическом направлении и приобретает стратегическое значение в процессе развития и обучения. Данный курс способствует развитию инженерного мышления и усовершенствованию практических навыков, предоставляя учащимся знания о современных инструментах для решения

разнообразных кейсов в области искусственного интеллекта.

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 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.

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 программы 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.

Возраст обучающихся, участвующих в реализации данной общеобразовательной программы: от 15 до 17 лет.

Зачисление в детское объединение происходит по заявлению родителей (законных представителей) обучающихся. Набор обучающихся в объединение – свободный. Наличие какой-либо специальной подготовки не требуется.

Сроки реализации программы: программа вводится с 11.11.2026 г. - всего 27 ч.

Формы обучения:

- викторина;
- демонстрация;
- квесты;
- разбор кейсов;
- лабораторно-практическая работа;
- игра;
- тренажеры.

Формы организации деятельности: занятия носят гибкий характер с учетом предпочтений, способностей и возрастных особенностей обучающихся. Построение занятия включает в себя фронтальную, индивидуальную и групповую работу.

Режим *занятий:* ***з***анятия проводятся 1 раз в неделю по 1 академическому часу (согласно санитарных требований к возрасту детей младшего школьного возраста).

Продолжительность учебного часа, согласно Прил. 3 СанПиН

2.4.4.3172-14, -40 мин., перерыв – 10 мин.

Наполняемость учебных групп: набор обучающихся проводится без предварительного отбора. Формирование групп от 20 человек.

Планируемые результаты обучения

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 научнотехнический 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 ИИгенерации 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 ИИконтента;

− 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.

Способы отслеживания результатов освоения программы учащимися:

– Педагогическое наблюдение в ходе выполнения практических заданий и проектной работы.

– Командные зачеты по разработке моделей и алгоритмов ИИ.

– Участие в практических заданиях, мини-проектах по созданию и улучшению моделей машинного обучения.

– Презентация своих мини-проектов и разработок на публику с анализом их эффективности.

Формы оценивания:

– Входной контроль – отсутствует, поскольку программа рассчитана на учащихся с разным уровнем подготовки.

– Промежуточный контроль – выполнение практических заданий и проектов по каждой теме программы. Контроль осуществляется через анализ результатов выполнения заданий по моделям и алгоритмам ИИ.

– Итоговый контроль – защита мини-проекта, в рамках которого учащиеся должны разработать и представить модель ИИ для решения конкретной задачи с применением изученных методов (регрессия, классификация, нейронные сети и ансамблевые методы).

Учебно-тематический план программы дополнительного образования
«Искусственный интеллект и информационная безопасность»

№ / акцент занятия		Темы занятия	Колво 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 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 ИИагенты. 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 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	1	Эволюция представлений об ИИ в литературе, кино и искусстве и их влияние на общественные ожидания и на сами исследования. Разграничение научной фантастики, футурологического	Анализировать эволюцию представлений об ИИ в литературе, кино и искусстве и их влияние на общественные ожидания и сами исследования.

		реальности		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.	Разграничивать научную фантастику, футурологический прогноз и реальную 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	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.

				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.	
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 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.	Объяснять криптографические основы пароля: пространство ключей, трудоемкость перебора, важность стойкости и уникальности. Характеризовать многофакторную и адаптивную аутентификацию: одноразовые коды, аппаратные ключи, 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. ИИсобеседники: чат-боты и ИИ-агенты в	Соблюдать сетевой этикет и правовые рамки общения в цифровой среде. Анализировать проблемы анонимности, верификации личности собеседника и доверия в открытых

				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.	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.
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,	Описывать дискретное представление изображений и звука: пиксель и цветовую модель, звуковой сигнал. Характеризовать распознавание речи и синтез голоса, оптическое

				компьютерное зрение, генерация изображений по описанию. Трудности распознавания (двусмысленность, ирония, шум в данных). Риск слежки и этические ограничения работы с биометрией.	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,	Раскрывать правовое содержание персональных данных: категории, основания и цели обработки, права субъекта и обязанности оператора. Описывать цифровой след и профиль

				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.	(cookie, метаданные, геолокацию, 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	Разбирать правовой смысл согласий и политик конфиденциальности, cookieуведомлений: 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

				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.	сервисах и обосновывать принятые решения.
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: чувствительность данных двойника, последствия неточной модели, вопрос доверия к решениям, принятым на основе модели.	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 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	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

				достоверности: верификация источника и перепроверка по независимому каналу.	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	Онлайнмошенничество: схемы, механизмы и порядок действий при инциденте	1	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	Классифицировать схемы онлайн-мошенничества: фишинг и 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

				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).	отказывать подозрительным.
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	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

				полученного результата с помощью возможностей ИИ; обобщение и проверка полученных результатов. Академическая честность: ответственность автора, риск делегирования мышления технологиям ИИ.	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. Правовые последствия действий подростков в сети с позиции уголовной ответственности: нарушение авторских и смежных прав (ст. 146 УК РФ).	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 ИИконтента. 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 аутентификация при проведении операций. Биометрия в финансовом доступе,	Описывать архитектуру защиты безналичных платежей: клиентсерверную модель и разделение зон ответственности, шифрование канала, протоколы подтверждения, многофакторную аутентификацию при операциях. Характеризовать биометрию в финансовом доступе (голосовую,

				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.	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. Проверка устройства антивирусом,	Классифицировать семейства и тактики вредоносного ПО: вирусы, черви, трояны, шпионское и рекламное ПО. Характеризовать средства защиты (антивирус, межсетевой экран, контроль приложений, обновления, резервное копирование) и настраивать их.

				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.	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	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.

				за критические решения.	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	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.

				беспилотником. Регуляторные требования к кибербезопасности критической инфраструктуры и авиационных систем; этические и правовые вопросы применения беспилотников.	
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,	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.

				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.	
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		

Содержание программы

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. ИИсобеседники: 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, cookieуведомления. 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 фитнесустройства 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, ИТспециальности 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.

Воспитательный компонент

Система воспитательной работы основывается на базовых принципах Стратегии развития воспитания в Российской Федерации на период до 2030 года. Воспитательная работа в объединении осуществляется в процессе формирования целостного коллектива с учѐтом индивидуальности каждого учащегося. Предусматривается участие в воспитательных мероприятиях школы, участие в конкурсных мероприятиях и проектах.

Обеспечение программы

Методическое обеспечение программы

Основные принципы, положенные в основу программы:

– принцип доступности, учитывающий индивидуальные особенности каждого обучающегося, создание благоприятных условий для их развития;

– принцип демократичности, предполагающий сотрудничество педагога и обучающегося;

– принцип системности и последовательности – знание в программе даются в определенной системе, накапливая запас знаний, дети могут применять их на практике.

Методы работы:

С точки зрения подачи учебного материла, на занятиях используются следующие методы:

– словесные методы (рассказ, беседа, инструктаж, чтение справочной литературы);
– наглядные методы (демонстрация мультимедийных презентаций, фильмов);
– практические методы (практические работы).

С точки зрения творческой активности обучающихся, используются следующие методы:

– репродуктивные методы (выполнение заданий по образцу);
– исследовательские методы (обучающиеся сами открывают необходимую информацию);
– эвристические методы (частично-поисковые, с возможностью выбора нескольких вариантов);
– проблемные методы (методы проблемного изложения, когда дается лишь часть готового задания).

Информационно-методическое обеспечение программы

– специализированная литература по информационным технологиям, подборка журналов;

– плакаты, фото и видеоматериалы;

– учебно-методические пособия для педагога и обучающихся, включающие, информационный и справочный материалы на различных носителях, компьютерное и видео оборудование;

– электронные учебники, справочные материалы, учебные задания, тесты.

Организационное обеспечение программы

В процессе обучения применяются различные формы организации учебной деятельности:

– беседы с фронтальным и индивидуальным устным и письменным опросом;

– лабораторно-практические и самостоятельные работы;

– учебные задания;

– проекты;

– презентации;

– игры.

Материально-техническое обеспечение программы

– 10 компьютерных столов и ноутбуков для обучающихся;

– ноутбук учителя;

– проектор с экраном;

– звуковые колонки;

– сканер;

– принтер;

– электронные носители информации.

Список литературы

1. Вьюгин В. В. «Математические основы машинного обучения и прогнозирования» - МЦНМО., 2013 г.

2. Бринк Х., Ричардс Д. «Машинное обучение» — Питер, 2017 г.

3. Бастиан Ш. «Крупномасштабное машинное обучение вместе с Python» - ДМК Пресс, 2017 г.

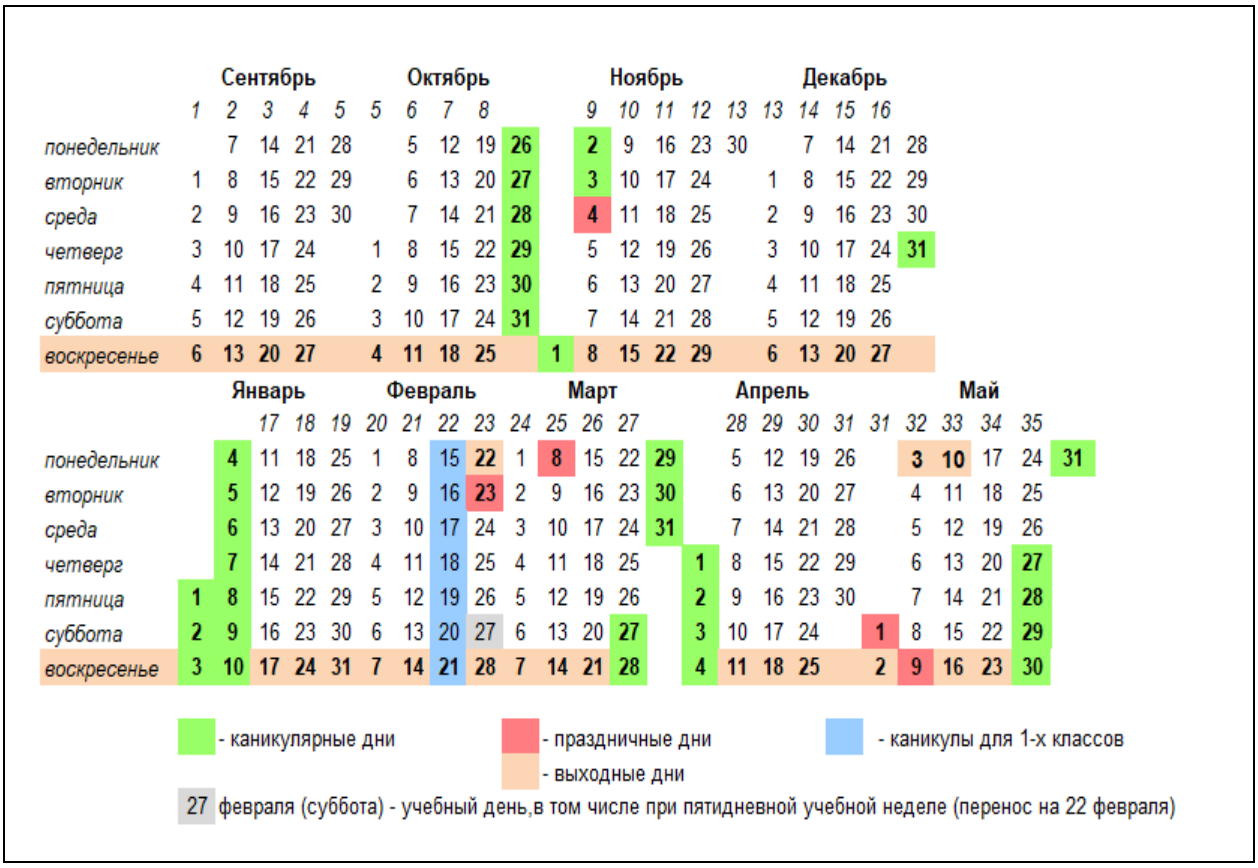
4. Г. А. Кухарев, Е. И. Каменская, Ю. Н. Матвеев, Н. Л. Щеголева «Методы обработки и распознавания изображений лиц в задачах биометрии» — Санкт-Петербург, Вильямс, 2013 г.

5. Флах П. «Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных» — ДМК Пресс, 2017 г.

6. Кузнецов, И.Н. Основы научных исследований / И.Н. Кузнецов – М.: Издательско-торговая корпорация «Дашков и К°», 2017 – 283 с.

ПРИЛОЖЕНИЕ

Годовой календарный учебный график ГБОУ СОШ №11 г. Кинеля на 2026-2027 учебный год



	Сентябрь					Октябрь					Ноябрь					Декабрь				
	1	2	3	4	5	5	6	7	8		9	10	11	12	13	13	14	15	16	
понедельник		7	14	21	28		5	12	19	26	2	9	16	23	30		7	14	21	28
вторник	1	8	15	22	29		6	13	20	27	3	10	17	24		1	8	15	22	29
среда	2	9	16	23	30		7	14	21	28	4	11	18	25		2	9	16	23	30
четверг	3	10	17	24		1	8	15	22	29	5	12	19	26		3	10	17	24	31
пятница	4	11	18	25		2	9	16	23	30	6	13	20	27		4	11	18	25	
суббота	5	12	19	26		3	10	17	24	31	7	14	21	28		5	12	19	26	
воскресенье	6	13	20	27		4	11	18	25		1	8	15	22	29	6	13	20	27	

	Январь					Февраль					Март					Апрель					Май				
	17	18	19	20	21	22	23	24	25	26	27		28	29	30	31	31	32	33	34	35	
понедельник	4	11	18	25	1	8	15	22	1	8	15	22	29		5	12	19	26		3	10	17	24	31
вторник	5	12	19	26	2	9	16	23	2	9	16	23	30		6	13	20	27		4	11	18	25	
среда	6	13	20	27	3	10	17	24	3	10	17	24	31		7	14	21	28		5	12	19	26	
четверг	7	14	21	28	4	11	18	25	4	11	18	25		1	8	15	22	29		6	13	20	27	
пятница	1	8	15	22	29	5	12	19	26	5	12	19	26	2	9	16	23	30		7	14	21	28	
суббота	2	9	16	23	30	6	13	20	27	6	13	20	27	3	10	17	24		1	8	15	22	29	
воскресенье	3	10	17	24	31	7	14	21	28	7	14	21	28	4	11	18	25		2	9	16	23	30	

- каникулярные дни
- праздничные дни
- каникулы для 1-х классов
- выходные дни

27 февраля (суббота) - учебный день,в том числе при пятидневной учебной неделе (перенос на 22 февраля)