Муниципальное автономное общеобразовательное учреждение
города Новосибирска «Лицей № 9»

Рабочая программа

Наименование курса внеурочной деятельности: **Информационная безопасность, Искусственный интеллект**

Классы: **8-10 классы**

Срок реализации программы, учебные годы, количество часов по учебному плану:

Учебные годы	Количество часов в год/ в неделю
	8 – 10 класс
2025-2026 уч.г.	68/ 2

Программа составлена на основе:

Федерального государственного образовательного стандарта ООО, Основной образовательной программы МАОУ «Лицей № 9» СОО,

Учебные пособия: Информационная безопасность. 10-11 классы. Учебник. Правовые основы информационной безопасности. 2021. Учебник. Цветкова М.С.; Онлайн-курс при поддержке Академии искусственного интеллекта для школьников, экспертов Физтех-школы прикладной математики и информатики МФТИ и Фонда развития Физтех-школ

Рабочую программу составил: _____ / Кольцова М.Н.
подпись расшифровка подписи

Новосибирск, 2025

Рабочая программа учебного курса разработана в соответствии с требованиями обновлённого Федерального государственного образовательного стандарта основного общего образования (ФГОС ООО), учитывает требования к предметным (образовательные области «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»), метапредметным и личностным результатам, а также программы воспитания.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебный курс «Информационная безопасность» и «Искусственный интеллект» использует воспитательные возможности содержания учебных предметов «Информатика» и «Основы безопасности жизнедеятельности». Курс направлен для подготовки учащихся к Олимпиаде НТО и другим конкурсам и олимпиадам по данным профилям и включает себя два направления: «Информационная безопасность» и «Искусственный интеллект».

«Искусственный интеллект» (базовый) носит междисциплинарный и комплексный характер. С одной стороны, в нем синтезируются знания и умения учащихся, полученные ими на уроках математики, информатики, физики, биологии (решение задач с физическим и/ или биологическим содержанием). С другой стороны, в структуре этого курса отчетливо выделяются и теоретическая и практическая составляющие. Учащиеся знакомятся с областями применения и базовыми понятиями курса, а в ходе дидактических игр и выполнения практических и проектных заданий получают опыт активной, творческой индивидуальной, групповой и коллективной деятельности по осмыслению ключевых задач машинного обучения и основных подходов в применении машинного обучения для создания интеллектуальных систем.

Цель курса: подготовить учащихся к Олимпиаде НТО по данным направлениям, также для различных Олимпиад по данным профилям, обеспечить социальные аспекты информационной безопасности в воспитании школьников в условиях цифрового мира, формирование навыков анализа данных, включение цифровой гигиены в контекст воспитания детей на регулярной основе, формирование у выпускника школы правовой

грамотности по вопросам информационной безопасности, которые влияют на социализацию детей в информационном обществе, формирование личностных и метапредметных результатов обучения и воспитания детей. Задачи курса по информационной безопасности и искусственному интеллекту:

– формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как человеческая жизнь, свобода, равноправие и достоинство людей, здоровье, опыт гуманных, уважительных отношений с окружающими; – создавать педагогические условия для

- формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствий деструктивных действий,

- формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения; – формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет; – мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими моральноправовых регуляторов жизни общества и государства в условиях цифрового мира;

– научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира,

- осознавать ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества

- развитие у учащихся устойчивого интереса к освоению данной области знаний и формирование представления о многообразии подходов в разработке искусственного интеллекта, об их возможностях и ограничениях, приобретение базовых знаний и умений в сферах науки о данных, машинного обучения и многообразии сфер их применения, а также формирование цифровой грамотности,

- развитие компетенций в области искусственного интеллекта, востребованных на отечественном рынке труда с учетом динамично развивающейся сферы ИИ

МЕСТО УЧЕБНОГО КУРСА В УЧЕБНОМ ПЛАНЕ

Рабочая программа курса составлена с использованием пособий «Информационная безопасность. Безопасное поведение в сети Интернет» Цветкова М. С., Якушина Е. В. – Издательство: Просвещение, 2022 г., «Информационная безопасность. Кибербезопасность» Цветкова М. С., Якушина Е. В. – Издательство: Просвещение, 2023 г., также Онлайн-курс при поддержке Академии искусственного интеллекта для школьников, экспертов Физтех-школы прикладной математики и информатики МФТИ и Фонда развития Физтех-школ

В соответствии с Учебным планом МАОУ «Лицей №9» курс рассчитан в 8и, 9и, 10 и, классе – на 68 ч (17 учебные недели). Количество часов в неделю составляет по 2 часа в 8-10 классах. В 1 полугодии изучается «Иноформационная безопасность», 2 полугодие «Искусственный интеллект».

Планируемые результаты изучения курса

Личностные

● сформированность основ саморазвития и самовоспитания в соответствии с

общечеловеческими ценностями и идеалами гражданского общества; готовность и способность

к самостоятельной, творческой и ответственной деятельности;

● толерантное сознание и поведение в поликультурном мире, готовность и способность

вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и

сотрудничать для их достижения, способность противостоять идеологии экстремизма,

национализма, ксенофобии, дискриминации по социальным, религиозным, расовым,

национальным признакам и другим негативным социальным явлениям;

● навыки сотрудничества со сверстниками, детьми младшего возраста, взрослыми в образовательной, общественно полезной, учебно-исследовательской, проектной и других видах деятельности;

● нравственное сознание и поведение на основе усвоения общечеловеческих ценностей;

● готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности;

● осознанный выбор будущей профессии и возможностей реализации собственных жизненных планов; отношение к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных проблем;

● принятие и реализацию ценностей здорового и безопасного образа жизни правил индивидуального и коллективного безопасного поведения в информационно телекоммуникационной среде.

Предметные

Выпускник научится:

● безопасно использовать средства коммуникации;

● безопасно использовать ресурсы интернета;

● идентифицировать типичные инциденты;

● задавать базовые параметры, в том числе параметры защиты от несанкционированного

доступа к операционным системам;

● настраивать и управлять сетевыми устройствами;

● использовать процедуры восстановления данных;

● определять точки восстановления данных;

● производить мониторинг администрируемых сетевых устройств информационнокоммуникационных систем;

● применять внешние программно-аппаратные средства для контроля

производительности сетевой инфраструктуры;

● устанавливать и настраивать параметры сетевых протоколов, реализованных в телекоммуникационном оборудовании;

● применять программно-аппаратные средства защиты информации в операционных системах;

● применять антивирусные средства защиты информации в операционных системах;

● анализировать компьютерную систему с целью определения уровня защищенности;

● использовать типовые криптографические средства защиты информации;

● классифицировать и оценивать угрозы информационной безопасности;

● изготавливать защищенное техническое средство или систему обработки информации.

Выпускник овладеет:

● основами правовых аспектов использования компьютерных программ и работы в Интернете;

● представлениями о влиянии информационных технологий на жизнь человека в обществе;

● знаниями об "операционных системах" и основных функциях операционных систем;

● знаниями об общих принципах разработки и функционирования интернет-приложений;

● представлениями о компьютерных сетях и их роли в современном мире;

● приемами безопасной организации своего личного пространства данных с

использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

● навыками и умениями безопасного и целесообразного поведения при работе с

компьютерными программами и в Интернете;

● основными навыками и умениями использования компьютерных устройств.

Выпускник получит возможность овладеть:

● навыками инженерного мышления;

● навыками работы с реальными программно-аппаратными комплексами;

● навыками оценивания уровня безопасности компьютерных систем; навыками

обеспечения информационной безопасности личного пространства;

● различными источниками информации, включая Интернет-ресурсы и другие базы данных для решения коммуникативных задач в области безопасности жизнедеятельности.

Метапредметные

● умение самостоятельно определять цели деятельности и составлять планы

деятельности; самостоятельно осуществлять, контролировать и корректировать деятельность; использовать все возможные ресурсы для достижения поставленных целей и реализации планов деятельности; выбирать успешные стратегии в различных ситуациях;

● умение продуктивно общаться и взаимодействовать в процессе совместной

деятельности, учитывать позиции других участников деятельности, эффективно разрешать конфликты;

● владение навыками познавательной, учебно-исследовательской и проектной деятельности, навыками разрешения проблем; способность и готовность к самостоятельному поиску методов решения практических задач, применению различных методов познания;

● готовность и способность к самостоятельной информационно-познавательной деятельности, владение навыками получения необходимой информации из словарей разных типов, умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников;

● умение использовать средства информационных и коммуникационных технологий (далее - ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;

● умение определять назначение и функции различных социальных институтов;

● умение самостоятельно оценивать и принимать решения, определяющие стратегию

поведения, с учетом гражданских и нравственных ценностей;

● владение языковыми средствами - умение ясно, логично и точно излагать свою точку зрения, использовать адекватные языковые средства;

● владение навыками познавательной рефлексии как осознания совершаемых действий и мыслительных процессов, их результатов и оснований, границ своего знания и незнания, новых познавательных задач и средств их достижения

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА

Рабочей программой предусмотрен следующий тематический план, который представлен в таблице 1. Таблица 1. Тематический план.

/п	**Модуль**	**Наименование раздела**	**Количество часов**
.	Введение в информационную безопасность	Основы Информационной безопасности.	2
.		Направления обеспечения информационной безопасности	2
.		Защита информации методами симметричного шифрования	2
.		Стеганография	2
.		Основы теории чисел	2
.	Элементы информационной безопасности в вычислительных сетях	Криптография	2
.		Вычислительные сети	2
.	Элементы информационной безопасности программного обеспечения	Основы операционных систем	2
·		Законодательство в сфере информационной безопасности	2
0.		Вредоносные программы	2
1.	Элементы защиты информации в вычислительных системах	Программно-технические средства защиты информации	2
2.		Социальная инженерия	2
3.		Анализ безопасности веб-проектов	2

4.		Процессы, связанные с обеспечением защиты данных	2
5.		Обеспечение безопасности вычислительных сетей	2
6.		Эшелонированная оборона	2
7.		Интернет вещей	2
	Итого		34

Краткое содержание разделов

Раздел 1. Основы Информационной безопасности. Что представляет собой кибербезопасность и почему потребность в специалистах по кибербезопасности продолжает расти. Что такое организационные данные и почему их важно защищать? Кто такие киберпреступники и что им нужно. Рассматриваются примеры атак, нарушений безопасности, а так же цели защиты. Разбор некоторых примеров атак на информационные системы.

Раздел 2. Направления обеспечения информационной безопасности.

Технические каналы утечки информации: технический, электромагнитный, оптический. Средства защиты от технических угроз. Экономическая модель защиты информации.

Раздел 3. Защита информации методами симметричного шифрования. Симметричные шифры: шифры древней спарты, шифр Брайля, атбаш, Цезаря, Гросфельда, Виженера, вертикальной перестановки, афинный шифр, шифр Хилла, Плейфера, Вернама.

Представление информации в формате BASE64

Раздел 4. Стеганография. Исторический обзор стеганографических систем. Описание стеганографических систем. Основные угрозы и типы нарушителей безопасности стеганографических систем. Типы атак на различные стеганографические системы.

Раздел 5. Основы теории чисел. Целые числа, простые числа, позиционные системы счисления. Сравнения по модулю. Уравнения в целых числах. Теория множеств, множества и функции, комбинаторика, вероятность и случайность. **Криптография.** Криптоанализ симметричных шифров. Статистическая устойчивость шифротекстов. Односторонние функции. Передачи зашифрованных сообщений и ключей шифрования по открытым каналам связи. Хеш функции. **Вычислительные сети.** Виды сетей, топология сетей, компоненты сетей. Сетевая модель OSI. Введение в Packet Tracer и создание виртуальных сетей. Защита вычислительных сетей от внешних и внутренних угроз. Виртуальные частные и анонимные сети.

Раздел 6. Основы операционных систем. Архитектура вычислительных машин. Язык Ассемблер. Основы администрирования Операционных систем Windows и Linux. Установка и настройка специальных операционных систем

Раздел 7. Законодательство в сфере информационной безопасности.

Авторское право и лицензии. Коммерческая тайна и способы ее защиты. Персональные данные и правила обращения с ними.

Раздел 8. Вредоносные программы. Классификация вредоносных программ:

Троянская программа, Вирус, Червь, программы шпионы, рекламные программы.

Раздел 9. Программно-технические средства защиты информации.

Антивирусные программы и принципы их работы.

Раздел 10. Социальная инженерия. Сбор информации и профайлинг. Доксинг.

Методы социальной инженерии.

Раздел 11. Анализ безопасности веб-проектов. Техники аудита безопасности вебпроектов. Общие знания относительно рисков, сопровождающих современные интернетприложения. Методики анализа безопасности клиент-серверных приложений. Методики анализа кода. Архитектурный анализ.

Раздел 12. Процессы, связанные с обеспечением защиты данных. Сертификаты. LDAP. RADIUS. Kerberos. Контроль доступа. Методы обеспечения процессов авторизации и учета.

Раздел 13. Обеспечение безопасности вычислительных сетей. Контроль сетевого трафика. Архитектура безопасной сети. Защита беспроводных сетей.

Раздел 14. Эшелонированная оборона. Безопасность системы и приложений, Основные правила для защиты операционных систем и отключение ненужных компонентов системы. Настройка локальных браундмаеров. Управление правилами приложений.

Раздел 15. Интернет вещей. Что такое интернет вещей. Безопасность трафика, генерируемого интернетом вещей. Безопасность интернет вещей. Интернет вещей в бизнесе и на предприятиях. Автоматизация посредством интернет вещей.

СОДЕРЖАНИЕ ОБУЧЕНИЯ

Модуль 1.Массивы в Python.

Тема 1.1. Этапы решения задачи на компьютере. Линейный алгоритм, блок-схема. Математические операторы, оператор присваивания, функции print(), input(), float(). Этапы решения задач на компьютере. Модель, алгоритм, формализация, линейный и разветвляющийся алгоритмы. Условный оператор в Python, полный и неполный условные операторы.

Тема 1.2. Решение задач на компьютере. Повторение основных базовых понятий Python, изученных ранее.

Тема 1.3. Одномерные массивы в Python - списки. Создание списков и вывод элементов. Список, массив, элементы списка, индекс элемента списка. Методы .append и .sort, положительные и отрицательные индексы, срезы.

Тема 1.4. Исследование и генерация списков. Вычисление суммы элементов списка. Методы .append и .sort, функции min(), max() и метод .count. Суммирование элементов списка, цикл с заданным числом повторений, оператор for. Генерация списка, операторы for и if.

Тема 1.5. Словари и их описание. Поиск по словарю. Списки, генерация списков, суммирование элементов списка, функция len(), сложение списков. Словари, элементы словаря, ключ и значение, вывод элементов словаря, поиск элементов в словаре.

Тема 1.6. Перебор элементов словаря. Словарь, список, операторы for и if, элемент словаря, ключ, значение, перебор словаря по ключам, перебор словаря по значениям, методы .keys, .values, .items, операторы for и if.

Тема 1.7. Решение задач с использованием списков и словарей. Список, срез, положительная и отрицательная индексация элементов списка, метод .append. Генерация списка, операторы for и if. Словарь, элементы словаря, ключи и значения, вложенные словари, метод .items. Тема 1.8. Повторение. Итоговая работа «Массивы в Python». Основные понятия модуля 1: списки и словари».

2. Машинное обучение.

Тема 2.1. Понятие и виды машинного обучения. Искусственный интеллект, подход, основанный на правилах, машинное обучение. История развития ИИ в играх, сферы применения машинного обучения. Обучение с учителем, обучение без учителя, задача

регрессии, задача классификации, задача кластеризации, отбор данных для модели машинного обучения.

Тема 2.2. Анализ и визуализация данных. Машинное обучение с учителем, машинное обучение без учителя. Задача регрессии, задача классификации, задача кластеризации. Библиотеки pandas и matplotlib, чтение табличных данных, статистические показатели, построение диаграмм.

Тема 2.3. Библиотеки машинного обучения. Машинное обучение с учителем и без учителя, его преимущества. Постановка цели и задач, анализ данных, обучающая и тренировочная выборки, задача регрессии, задача классификации, тестовая и тренировочная выборка, переобучение, недообучение, оптимальная модель, кросс-валидация. Библиотека sklearn, этапы построения модели машинного обучения на Python.

Тема 2.4. Линейная регрессия. Понятие линейной регрессии, целевая функция, линейное уравнение, гомоскедастичность данных. Создание модели линейной регрессии на Python с помощью библиотек pandas, numpy и sklearn.

Тема 2.5. Нелинейные зависимости. Создание, обучение и оценка модели линейной регрессии. Визуализация данных на Python. Нелинейный функции, графики функций. Полиномиальное преобразование линейной регрессии.

Тема 2.6. Классификация. Логистическая регрессия. Классификация, логистическая регрессия, линейный классификатор, гиперплоскость, бинарная классификация, мультиклассовая классификация. Линейное уравнение, коэффициенты линейного уравнения, расположение точки относительно прямой, отступ объекта. Создание, обучение и оценка модели логистической регрессии.

Тема 2.7. Классификация. Логистическая регрессия. Матрица ошибок, метрики качества логистической регрессии, модель логистической регрессии на Python.

Тема 2.8. Деревья решений. Часть 1. Дерево решений, элементы деревьев: корень, листья; глубина дерева, жадный алгоритм, атрибут разбиения; энтропия, формула Шеннона, вероятность, критерий Джини.

Тема 2.9. Деревья решений. Часть 2. Методы решения проблемы переобучения деревьев. Модели дерева решений.

Реализация дерева решения на Python.

Тема 2.10. Проект «Решение задачи классификации». Машинное обучение с учителем, задача классификации. Метрики оценки качества классификации. Этапы разработки модели машинного обучения, анализ данных, создание и обучение модели, оценка эффективности работы модели.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ Искусственный интеллект

Иметь представления о многообразии подходов в разработке искусственного интеллекта, их возможностях и ограничениях; о машинном обучении и сферах его применения;

Уметь объяснять разницу между машинным обучением с учителем и без учителя.

Выявлять и формулировать задачи машинного обучения для различных сфер жизни человека и в соответствии с реальными потребностями.

Иметь представления о создании модели классификации на сервисе Teachable Machine.

Иметь представления о недообученных и переобученных моделях машинного обучения, уметь выявлять проблемы по характерным признакам и знать способы борьбы с переобучением и недообучением моделей.

Получить практический опыт тестирования готовой модели машинного обучения

Иметь представления о сущности работы модели логистической регрессии и возможностях ее применения для классификации объектов; об использовании деревьев решений в машинном обучении.

Уметь создавать модели линейной регрессии на Python с помощью библиотек pandas, numpy и sklearn Уметь проектировать и реализовывать модели машинного обучения на Python с помощью инструментов библиотеки sklearn

Поурочно-тематическое планирование 1 полугодие «Информационная безопасность»

№	Тема урока	Часов	ЦОР	ФОРМА
1	Основы Информационной безопасности.	2	https://education.tbank.ru/school/generation/infosec/	Вводное занятие
2	Направления обеспечения информационной безопасности	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
3	Защита информации методами симметричного шифрования	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
4	Стеганография	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
5	Основы теории чисел	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
6	Криптография	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
7	Вычислительные сети	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
8	Основы операционных систем	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
9	Законодательство в сфере информационной безопасности	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
10	Вредоносные программы	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
11	Программно-технические средства защиты информации	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
12	Социальная инженерия	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
13	Анализ безопасности веб-проектов	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
14	Процессы, связанные с обеспечением защиты данных	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
15	Обеспечение безопасности вычислительных сетей	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
16	Эшелонированная оборона	2	https://education.tbank.ru/school/generation/infosec/	Практическая работа
	Итого	32		

2 полугодие «Искусственный интеллект»

№	Тема урока	Часов	ЦОР	ФОРМА
1.	Интернет вещей	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Вводное занятие
2.	Понятие и виды машинного обучения.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
3.	Искусственный интеллект, подход, основанный на правилах, машинное	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа

	обучение.			
4.	История развития искусственного интеллекта в играх, сферы применения машинного обучения.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
5.	Обучение с учителем, обучение без учителя, задача регрессии, задача классификации, задача кластеризации, отбор данных для модели машинного обучения.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
6.	Анализ и визуализация данных.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
7.	Машинное обучение с учителем, машинное обучение без учителя.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
8.	Задача регрессии, задача классификации, задача кластеризации.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
9.	Библиотеки pandas и matplotlib, чтение табличных данных, статистические показатели, построение диаграмм.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
10.	Библиотеки машинного обучения.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
11.	Машинное обучение с учителем и без учителя, его	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
12.	Постановка цели и задач, анализ данных, обучающая и тренировочная выборки, задача регрессии, задача классификации, тестовая и тренировочная выборка, переобучение, недообучение, оптимальная модель, кроссвалидация.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
13.	Библиотека sklearn, этапы построения модели машинного обучения на Python.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
14.	Понятие линейной регрессии.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
15.	Целевая функция, линейное уравнение, гомоскедастичность данных.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
16.	Создание модели линейной регрессии на Python с помощью библиотек pandas, numpy и sklearn.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
17.	Нелинейные зависимости.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Вводное занятие
18.	Создание, обучение и оценка модели линейной регрессии.	1	https://ai-academy.ru/teachers/courses/vvodnyj-	Практическая работа

			kurs-vvedenie-v-ii/promo/	
19.	Визуализация данных на Python.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
20.	Нелинейный функции, графики функций.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
21.	Полиномиальное преобразование линейной регрессии.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
22.	Классификация, логистическая регрессия, линейный классификатор, гиперплоскость, бинарная классификация, мультиклассовая классификация.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
23.	Линейное уравнение, коэффициенты линейного уравнения, расположение точки относительно прямой, отступ объекта.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
24.	Создание, обучение и оценка модели логистической регрессии.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
25.	Матрица ошибок, метрики качества логистической регрессии, модель логистической регрессии на Python.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
26.	Деревья решений.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
27.	Дерево решений, элементы деревьев: корень, листья; глубина дерева, жадный алгоритм, атрибут разбиения.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
28.	Энтропия, формула Шеннона, вероятность, критерий Джини.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
29.	Методы решения проблемы переобучения деревьев.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
30.	Модели дерева решений.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
31.	Реализация дерева решения на Python.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
32.	Проект «Решение задачи классификации».	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
33.	Машинное обучение с учителем, задача классификации.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Вводное занятие
34.	Метрики оценки качества классификации.	1	https://ai-academy.ru/teachers/courses/vvodnyj-kurs-vvedenie-v-ii/promo/	Практическая работа
35.	Этапы разработки модели машинного обучения, анализ	2	https://ai-academy.ru/teachers/courses/vvodnyj-	Практическая работа

	данных, создание и обучение модели, оценка эффективности работы модели.		kurs-vvedenie-v-ii/promo/	
	Итого	36		

Список учебной и методической литературы, и другие источники:

1. Абросимов, Л. И. Базисные методы проектирования и анализа сетей ЭВМ : учебное пособие / Л. И. Абросимов. — Санкт-Петербург : Лань, 2021. — 212 с. — ISBN 978-5-8114-3538-

8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/169320 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

2. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278. — Загл. с экрана.

3. Введение в сетевые технологии - https://stepik.org/course/58678/info

4. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры /

А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 261 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. — Режим доступа : www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1.

5. Вьюненко, Л. Ф. Имитационное моделирование : учебник и практикум для академического бакалавриата / Л. Ф. Вьюненко, М. В. Михайлов, Т. Н. Первозванская ; под ред. Л. Ф. Вьюненко. — М. : Издательство Юрайт, 2016. — 283 с. — (Бакалавр. Академический курс). — ISBN 978-59916-6428-8. [Электронный ресурс]— Режим

доступа: https://www.biblioonline.ru/book/BEE05A5A1AB0-4A08-ADB1-70BC357B6C20— Загл. с экрана.

6. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум : учебное пособие / Р. Н. Гилязова. — Санкт-Петербург : Лань, 2020. — 44 с. — ISBN 978-5-8114-4294-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130179 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

7. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография - М.: Солон-Пресс, 2017. — 262 с. — ISBN 978-5-91359-173-9.

8. Давидюк Н.В. Обеспечение безопасности абонентского телетрафика путём конфигурирования и настройки маршрутизатора (на примере MikroTik RouterBOARD) - Практикум. — СПб.: Интермедия, 2020. — 68 с. — ISBN 978-5-4383-0195-0

9. Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

10. Журавлев, А. Е. Инфокоммуникационные системы: протоколы, интерфейсы и сети. Практикум : учебное пособие для спо / А. Е. Журавлев. — Санкт-Петербург : Лань, 2020. — 192 с. — ISBN 978-5-8114-5633-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152624 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

11. Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 392 с. — ISBN 978-5-8114-8514-7. — Текст : электронный // Лань : электроннобиблиотечная система. — URL: https://e.lanbook.com/book/176657 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

12. Журавлев, А. Е. Инфокоммуникационные системы. Программное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 376 с. — ISBN 978-5-8114-8515-4. — Текст : электронный // Лань : электроннобиблиотечная система. — URL: https://e.lanbook.com/book/176658 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

13. Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электроннобиблиотечная система. — URL: https://e.lanbook.com/book/111057 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

14. Кибербезопасность: что нужно знать о новом виде защиты? - https://stepik.org/course/69690/syllabus

15. Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие для вузов / В. Г. Кобылянский. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 120 с. — ISBN 978-5-8114-8187-3. — Текст : электронный // Лань : электронно-библиотечная

система. — URL: https://e.lanbook.com/book/173109 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

16. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-81145632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

17. Кутузов, О. И. Инфокоммуникационные системы и сети : учебник для вузов / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 244 с. — ISBN 978-5-8114-8051-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171410 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

18. Лившиц И.И. Нормативно-методическое обеспечение информационной безопасности - Учебно-методическое пособие. – СПб: Университет ИТМО, 2021. – 68 с.

19. Маркина Т.А. Основные механизмы защиты в ОС MS Windows. Методические рекомендации по выполнению лабораторных работ - СПб.: Университет ИТМО, 2020. — 34 с.

20. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. — Санкт-Петербург : Лань, 2020. — 456 с. — ISBN 978-5-8114-4424-3. — Текст :

электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/140740 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

21. Математика в кибербезопасности - https://stepik.org/course/62247/syllabus

22. Молдовян А.А., Молдовян Д.Н., Левина А.Б. Молдовян А.А., Молдовян Д.Н., Левина А.Б.

Протоколы аутентификации с нулевым разглашением секрета. – СПб: Университет ИТМО, 2016.

http://books.ifmo.ru/file/pdf/1887.pdf

23. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

24. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 96 с. — ISBN 978-5-8114-7906-1. — Текст : электронный // Лань : электронно-библиотечная система. —

URL: https://e.lanbook.com/book/167185 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

25. Никифоров, С. Н. Методы защиты информации. Защищенные сети : учебное пособие / С.

Н. Никифоров. — Санкт-Петербург : Лань, 2021. — 96 с. — ISBN 978-5-8114-3099-4. — Текст :

электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/169311 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

26. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 124 с. — ISBN 978-5-8114-8256-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/173803 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

27. Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 160 с. — ISBN 978-58114-4042-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114699 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

28. Новиков, В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс] : учебное пособие / В.К. Новиков. — Электрон. дан. — Москва : Горячая линия-Телеком, 2017. — 176 с. — Режим доступа: https://e.lanbook.com/book/111084. — Загл. с экрана.

29. Олифер, В.Г. Компьютерные сети принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. - М.: СПб: Питер, 2016. - 672

30. Операционные системы. Программное обеспечение : учебник. — Санкт-Петербург : Лань, 2020. — 248 с. — ISBN 978-5-8114-4290-4. — Текст : электронный // Лань : электроннобиблиотечная

система. — URL: https://e.lanbook.com/book/148222 (дата обращения: 13.07.2021).
— Режим доступа: для авториз. пользователей.

31. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 108 с. — ISBN 978-5-8114-8370-9. — Текст : электронный // Лань : электроннобиблиотечная система. — URL: https://e.lanbook.com/book/175506 (дата обращения: 13.07.2021).
— Режим доступа: для авториз. пользователей.

32. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для спо / В. И. Петренко, И. В. Мандрица. — Санкт-Петербург : Лань, 2021. — 108 с. — ISBN 978-5-8114-6924-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/153678 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

33. Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 124 с. — ISBN 9785-8114-7970-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/169817 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

34. Райтман М.А. Искусство легального анонимного и безопасного доступа к ресурсам Интернета. /Райтман М.А. Россия, БХВ-Петербург, 2017. ISBN 9785977537452 - 624 стр.

35. Сергеев, А. Н. Основы локальных компьютерных сетей : учебное пособие для спо / А. Н. Сергеев. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-6483-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148024 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

36. Советов, Б. Я. Моделирование систем: учебник для академического бакалавриата / Б. Я. Советов, С. А. Яковлев. — 7-е изд. — М. : Издательство Юрайт, 2017. — 343 с. — (Бакалавр. Академический курс). — ISBN 978-5-9916-3898-2.

37. Староверова, Н. А. Операционные системы : учебник для спо / Н. А. Староверова. — Санкт-Петербург : Лань, 2021. — 412 с. — ISBN 978-5-8114-6385-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/162376 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

38. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

39. Федосеев В.А. Цифровые водяные знаки и стеганография - 2-е изд., испр. и дополн. — Самара: Самарский университет, 2019. — 144 с. — ISBN 978-5-7883-1370-2

40. Хасанов Р.И. Основы стеганографии - Оренбург: Оренбургский государственный университет, 2017. — 102 с.

41. Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/132242 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

42. Marion Nancy E., Twede Jason. Cybercrime: An Encyclopedia of Digital Crime - ABC-CLIO, LLC., 2020. — 485 p. — 978-1-4408-5735-5

43. Калинин И. А. / Самылкина Н. Н. / Салахова А.А. Информатика 10-11

44. Калинин, Самылкина, Салахова: Искусственный интеллект. 10-11 классы. Учебное пособие. ФГОС

45.