Министерство образования Края
Филиал АНО ДТ «Красноярский «Кванториум» в г. Норильске
«Центр цифрового образования детей IT-Куб г. Норильск»

СОГЛАСОВАНО:
Заведующая учебной частью
_____ Д.С. Симашова
протокол № 13
от «02» 09 2026 г.

УТВЕРЖДАЮ:
Директор филиала
_____ Е. С. Тадер
Приказ № 02-02-94
от «02» 09 2026 г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА НА 2026-2027 уч.год
технической направленности

«Кибергигиена и нейросети»

Форма реализации: очная
Срок реализации: 1 год
Возраст детей: 12-14 лет

Составитель программы:
Бихтор Леонид Андреевич
педагог дополнительного образования

г. Норильск, 2026 г.

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная общеобразовательная общеразвивающая программа «Кибергигиена и нейросети» (далее – программа) имеет техническую направленность и разработана в соответствии с основными нормативно-правовыми документами:

- ✓ Федеральный закон «Об образовании» от 29.12.2012 № 273-ФЗ;
- ✓ Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ;
- ✓ Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ;
- ✓ Указ Президента Российской Федерации «О национальных целях развития Российской Федерации на период до 2030 года»;
- ✓ Концепция развития дополнительного образования до 2030 года (утверждена распоряжением Правительства РФ от 31.03.2022 № 678-р);
- ✓ Стратегия развития воспитания в Российской Федерации на период до 2025 года (утверждена распоряжением Правительства Российской Федерации от 29.05.2015 № 996-р);
- ✓ План мероприятий по реализации в 2021 - 2025 годах «Стратегии развития воспитания в Российской Федерации на период до 2025 года» (утвержден распоряжением Правительства Российской Федерации от 12.11.2020 № 2945-р);
- ✓ Приказ Министерства образования и науки Российской Федерации «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ» от 23.08.2017 № 816;
- ✓ Приказ Министерства Просвещения РФ «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам» от 09.11.2018 № 196;

- ✓ Приказ Министерства Просвещения РФ «Об утверждении Целевой модели развития региональных систем дополнительного образования детей» от 03.09.2019 № 467;
- ✓ Приказ Министерства Просвещения Российской Федерации «О внесении изменений в порядок организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам, утвержденный приказом Министерства Просвещения Российской Федерации от 09.11.2018 № 196» от 30.09.2020 № 533;
- ✓ Постановление Главного государственного санитарного врача РФ «Об утверждении СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи» от 28.09.2020 № 28;
- ✓ Распоряжение Правительства РФ "О мерах по обеспечению информационной безопасности в образовательных учреждениях" от 28.04.2023 № 1105-р;
- ✓ Письмо Министерства образования и науки РФ «О направлении информации» (с «Методическими рекомендациями по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы)» от 18.11.2015 № 09-3242.

Программа ориентирована на обучающихся в возрасте 12–14 лет. Основное внимание уделяется формированию у детей базовых знаний и практических навыков в области кибербезопасности и ответственного поведения в цифровой среде, освоению методов визуализации и анализа данных, а также знакомству с современными технологиями работы с нейросетями и их применением в повседневной жизни.

Программа способствует развитию технических и творческих способностей обучающихся, вовлекает их в исследовательскую и проектную деятельность. В процессе обучения дети осваивают не только предметные компетенции, но и универсальные навыки: работа в команде, взаимопомощь,

организаторские и лидерские качества, самостоятельность, ответственность и дисциплинированность.

Программа рассчитана на год и предусматривает общий объем занятий в 72 часа, по 2 академических часа в неделю.

1.1. АКТУАЛЬНОСТЬ ДООП

Кибергигиена и кибербезопасность становятся всё более важными в современном мире в связи с растущими угрозами, такими как хакерские атаки, вирусы и другие виды киберпреступности. Эти угрозы становятся всё более сложными и разнообразными, поэтому сегодня растёт осознание важности базовых навыков безопасности как среди взрослого населения, так и среди детей. Это, в свою очередь, приводит к совершенствованию методов защиты информации и компьютерных систем. Развитие технологий также повышает уровень цифровой уязвимости, что подчёркивает необходимость соблюдения мер кибергигиены и принятия эффективных мер по обеспечению кибербезопасности. С увеличением использования интернета и цифровых устройств особенно важно обучать школьников правилам безопасного поведения в сети, защите личных данных и предотвращению киберугроз. Понимание основных принципов кибербезопасности поможет детям избегать опасных ситуаций в онлайн-среде и формировать ответственное поведение в интернете.

Особое внимание в программе уделяется нейросетям и их практическому применению. Школьники знакомятся с принципами работы искусственного интеллекта, учатся использовать промпт-инжиниринг – искусство правильной постановки задач для нейросетей, что позволяет получать качественные, осмысленные и достоверные результаты. Эти навыки помогают школьникам не только в учёбе (подготовка материалов, поиск информации, творческие проекты), но и формируют базу для будущей профессиональной деятельности в цифровой экономике. Освоение

нейросетевых инструментов развивает критическое мышление, креативность и умение использовать современные технологии ответственно и эффективно.

Таким образом, программа готовит учащихся к вызовам современного информационного общества, сочетая основы кибербезопасности с освоением технологий искусственного интеллекта.

1.2 НОВИЗНА ДООП

Программа имеет несколько отличительных особенностей. Они включают в себя фокус на обучении безопасности в цифровом пространстве, учитывая защиту личных данных и предотвращение киберугроз в игровой форме. Также данный курс знакомит с основными категориями больших данных, со сферами генерации больших данных, с обучающимися будет рассматриваться опыт работы с большими данными в разных сферах деятельности и принципы работы с дынными, ребята даже попробуют себя в роли киберпреступников для лучшего понимания уязвимых сторон современного информационного пространства. Программа направлена на создание благоприятной обстановки для личностного роста студентов, их успешную социализацию, так как большая часть занятий направлена на общение обучающихся и работу в командах. Таким образом, курс будет представлять из себя не череду монотонных лекций, а работу со школьниками в интерактивном формате, для повышения эффективности изучения ребятами сложных тем, будут использовать медиа материалы собственного производства.

1.3 АДРЕСАТ ПРОГРАММЫ, ТРЕБОВАНИЯ К ОБУЧАЮЩИМСЯ

Набор на Программу осуществляется в соответствии с Положением о наборе в Филиал АНО ДТ «Красноярский «Кванториум» в г. Норильске «Центр цифрового образования детей IT-Куб г. Норильск». Обучающиеся, поступающие на программу, проходят собеседование, направленное на выявление их индивидуальности и склонности к выбранной деятельности.

Обучающиеся должны иметь базовые уровень пользования ПК, пакета Microsoft Office, начальный уровень знания английского языка.

В связи с ориентированностью программы на работу в малых группах и индивидуальный подход, оптимальное количество обучающихся в группе должно быть от 10 до 12 человек.

1.4. ПЕДАГОГИЧЕСКАЯ ЦЕЛЕСООБРАЗНОСТЬ

Дополнительная общеобразовательная общеразвивающая программа «Кибергигиена и нейросети» имеет техническую направленность, что позволяет обучающимся приобщиться к инженерно-техническим знаниям в области инновационных технологий, сформировать техническое мышление и научиться видеть достоверную информацию среди большого объема информации.

Изучив данную программу, обучающиеся овладеют навыками востребованных уже в ближайшие десятилетия специальностей, многие из которых включены в Атлас профессий будущего, таких как киберследователь, проектировщик личной безопасности, цифровой лингвист и т.д. В свете бурного развития технологий и цифровизации всех сфер жизни общества актуальность знаний и навыков, рассматриваемых в программе, будет только возрастать.

Данная образовательная программа помогает решать следующие актуальные педагогические задачи:

- развитие навыков работы с информацией в цифровой среде, включая умение эффективно и безопасно использовать различные онлайн-ресурсы и технологии;
- позволяет учащимся осознать риски и угрозы в онлайн-среде, развить навыки защиты личной информации, предотвращения кибератак и обеспечения безопасного поведения в интернете;

- ознакомление с вопросами этики и законности использования данных, что помогает школьникам понять важность соблюдения правил и норм в сфере цифровой безопасности;
- формирование необходимых навыков и знаний для успешной работы в сферах, связанных с кибербезопасностью, анализом данных и информационными технологиями, отвечая на актуальные запросы рынка труда;
- освоение базовых навыков промпт-инжиниринга — умения правильно формулировать запросы к нейросетям для получения качественных и полезных результатов;
- развитие критического мышления при работе с искусственным интеллектом, умение оценивать достоверность и корректность полученных данных;
- применение нейросетевых инструментов в учёбе и проектной деятельности (поиск информации, визуализация, творческие задания).

1.5. ОБЪЕМ/СРОК ОСВОЕНИЯ ПРОГРАММЫ

Программа рассчитана на 72 учебных часа. Срок освоения программы – учебный год, с сентября по май.

1.6. ЦЕЛИ И ЗАДАЧИ ПРОГРАММЫ

Цель дополнительной образовательной программы «Кибергигиена и нейросети» заключается в формировании у учащихся базовых знаний и практических навыков в области цифровой безопасности и ответственного поведения в сети, а также в освоении современных технологий работы с нейросетями. Программа направлена на развитие у школьников умения защищать личные данные, предотвращать киберугрозы, эффективно использовать цифровые инструменты, а также применять нейросети и промпт-инжиниринг для учёбы, творчества и проектной деятельности.

К основным задачам курса можно отнести:

1. Формирование умений к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, умения осуществлять целенаправленный поиск информации;

2. Изучение методов защиты своей личной информации, предотвращения кибератак, обнаружения и устранения уязвимостей в сетевых системах и приложениях;

3. Ознакомление с этическими и правовыми нормами, регулирующими использование информации и данных, а также в формировании у них навыков этичного поведения в цифровой среде;

4. Стимулирование самостоятельности и творческого подхода к решению повседневных задач;

5. Развитие основ коммуникативных отношений внутри коллектива;

6. Знакомство с принципами работы нейросетей и понимание их роли в современном мире;

7. Освоение основ промпт-инжиниринга – умения грамотно формулировать запросы к нейросетям для получения качественных результатов;

8. Развитие критического мышления при использовании ИИ, навыков оценки достоверности и корректности информации, получаемой от нейросетевых моделей;

9. Применение нейросетевых инструментов для учёбы, исследовательских проектов и творческих заданий, что способствует развитию универсальных учебных действий;

10. Формирование у школьников ответственности и культуры безопасного и осознанного использования современных цифровых технологий.

1.7. ФОРМА ОБУЧЕНИЯ, ВИДЫ ЗАНЯТИЙ И РЕЖИМ ЗАНЯТИЙ

Место реализации программы: Филиал АНО ДТ «Красноярский «Кванториум» в г. Норильске «Центр цифрового образования детей IT-Куб г.

Норильск». Адрес: ул. 50 лет Октября, д.10, г. Норильск, Красноярский край, 663305.

Срок реализации программы: Объем учебной нагрузки – 72 учебных часа.

Формы и режим занятий: Форма обучения – очная.

Режим занятий: 1 раз в неделю по 2 академических часа (1 академический час - 40 минут) с пятиминутным перерывом, что определяется санитарно-эпидемиологическими правилами и нормативами СП 2.4.3648-20.

При проведении занятий используются следующие формы работы:

- индивидуальная, обучающиеся могут работать над своими заданиями индивидуально;
- демонстрационная, когда обучающиеся слушают объяснения педагога и наблюдают за демонстрационным экраном или экранами компьютеров на ученических рабочих местах;
- коллективное обсуждение, в ходе которого дети могут делиться своими идеями, задавать вопросы и обсуждать различные аспекты верстки;
- групповая работа, когда ребята могут работать в микрогруппах, обмениваясь идеями, обсуждая проблемы и помогая друг другу при необходимости.

Обучение проводится в формате открытой беседы, где каждый обучающийся может высказать свое мнение по теме занятия. Практические занятия проходят в формате либо демонстраций для усвоения теоретического материала, либо игр, в ходе которых обучающие смогут в интересной форме изучить и укрепить новые знания и навыки.

1.8. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ

Результаты освоения программы «Кибергигиена и нейросети» должны соответствовать следующим пунктам:

- освоение знаний о базовых принципах безопасного поведения в сети, включая защиту личной информации, использование надежных паролей и определение подозрительных ситуаций;
- освоение современных методов защиты информации, включая основы шифрования, аутентификации, использование межсетевых экранов и других средств обеспечения кибербезопасности;
- понимание этических и правовых норм, касающихся использования цифровых технологий, и умение применять их в практической деятельности;
- осознание принципов работы нейросетей и понимание сфер их применения в повседневной жизни, учёбе и профессиональной деятельности;
- обретение базовых навыков промпт-инжиниринга – умения грамотно формулировать запросы для получения корректных и полезных результатов от нейросетей;
- формирование критического мышления и навыков анализа информации, включая оценку достоверности данных, получаемых с помощью искусственного интеллекта;
- наличие навыков коммуникации и сотрудничества в коллективе, необходимых для выполнения проектной и исследовательской работы;
- обретение умений самостоятельной организации своей деятельности, что создаёт основу для дальнейшего саморазвития и ответственного использования цифровых технологий.

1.9. ФОРМЫ ПОДВЕДЕНИЯ ИТОГОВ

Во время занятий текущий контроль освоения программы осуществляется через наблюдения, опросы и тестирования. Обучение разделено на несколько основных тем, по окончанию изучения которых обучающимся будет выдаваться контрольные работы в виде теста. Итоговая аттестация проводится в форме презентации финальной работы, которая

заключается в создании собственной памятки по пройденным темам курса (например, бумажная памятка, видео-урок, презентация и др.).

Финальная работа оценивается по следующим критериям:

1. Соответствие требованиям задания: проект должен полностью соответствовать поставленным требованиям и целям, указанным в исходном задании;

2. Оригинальность и креативность: оценивается оригинальность и креативность идеи оформления и подачи информации по пройденной программе, а также уровень творческого подхода к его выполнению;

3. Защита проекта: способность обучающегося ответить на вопросы и доступно и понятно представить свою работу.

2. УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№	Тема занятия	Количество часов			Формы аттестации/ контроля
		Всего	Теория	Практика	
Раздел 1. Введение (2 часа)					
1.1	Правила техники безопасности и санитарно-гигиенические нормы.	2	1	1	
Раздел 2. Основы кибергигиены (18 часов)					
2.1	Знакомство с основами безопасности.	2	1	1	
2.2	Фактчекинг. Зачем нам знать ложь изнутри?	2	1	1	
2.3	Основы работы с данными.	2	1	1	
2.4	Основы компьютерной грамотности.	10	5	5	
2.5	Текущий контроль по разделу «Основы кибергигиены».	2	0,5	1,5	Фронтальный опрос, тестирование.
Раздел 3. Цифровое пространство. (14 часов)					
3.1	Цифровой профиль: безопасность социальных сетей.	4	2	2	
3.2	Общение в сети.	2	1	1	
3.3	Поиск информации в сети.	6	2	4	
3.4	Текущий контроль по разделу «Цифровое пространство».	2	0,5	1,5	Фронтальный опрос, тестирование.
Раздел 4. Взлом и его последствия. (10 часов)					
4.1	Мошенничество.	4	2	2	
4.2	Пароли и шифрование.	2	1	1	

4.3	Вирусы и вредоносное ПО.	2	1	1	
4.4	Текущий контроль по разделу «Взлом и его последствия».	2	0,5	1,5	Фронтальный опрос, тестирование.
Раздел 5. Нейросети и искусственный интеллект. (20 часов)					
5.1	Введение в нейросети и ИИ	4	2	2	
5.2	Промпт-инжиниринг: как задавать вопросы нейросетям	4	2	2	
5.3	Применение ИИ в учёбе и проектах (генерация текста, изображений, видео, музыки идей)	8	2	6	
5.4	Культура использования ИИ: этика, правовые и социальные аспекты	2	2	0	
5.5	Текущий контроль по разделу «Нейросети и искусственный интеллект».	2	0,5	1,5	
Раздел 6. Разработка и защита итогового проекта (8 часов)					
6.1	Создание своей памятки по кибергигиене и работе с нейросетями.	6	1	5	
6.2	Защита проектов.	2	0	2	Теоретическое тестирование, защита проекта.
	ИТОГО	72	27	45	

3. СОДЕРЖАНИЕ ДООП

Раздел 1. Введение (2 часа)

Тема 1.1 Правила техники безопасности и санитарно-гигиенические нормы **(2 часа).**

Теория: Общие правила безопасности и поведения в учебном заведении. Инструкции по безопасному использованию оборудования и ПО. Правила пожарной безопасности. Действия в аварийных и чрезвычайных ситуациях. Требования к чистоте и порядку на рабочем месте.

Практика: Ознакомление с правилами техники безопасности через игровые ситуации и разбор примеров.

Раздел 2. Основы кибергигиены (18 часов)

Тема 2.1 Знакомство с основами безопасности **(2 часа).**

Теория: Основные понятия кибергигиены. Информационная безопасность. Знакомство с основами безопасности. Кто такие ИБ-специалисты.

Практика: Работа с новостями и ложной информацией. Игра «Шпион» - нужно вычислить среди 3 новостей ложную.

Тема 2.2 Фактчекинг. Зачем нам знать ложь изнутри? **(2 часа).**

Теория: Фактчекинг. Ложь изнутри. Как избежать ложную информацию.

Практика: Работа с ложной информацией, интерактивная деятельность «Час суда».

Тема 2.3 Понятие данных и как с ними работать. Жизненный цикл данных. Ответственность за данные. Культура обмена данных. **(2 часа).**

Теория: Введение в обработку информации, хранение и базовые инструменты для работы с данными.

Практика: Мини-задания на поиск и систематизацию информации.

Тема 2.4 Основы компьютерной грамотности **(10 часов).**

Теория: Знакомство и работа с прикладными программами для обработки информации. Знакомство с текстовым редактором. Работа с клавиатурой в текстовом редакторе. Изучение программ создания презентаций и их возможностями. Правила составления презентации. Работа в программе с электронными таблицами, построение диаграмм. Работа с Word, Excel, интернет-ресурсами.

Практика: Работа с прикладными программами для обработки информации (текстовые редакторы, создание презентаций, работа с электронными таблицами и диаграммами).

Текущий контроль по разделу «Основы кибергигиены» (**2 часа**, Приложение 1).

Раздел 3. Цифровое пространство (13 часов).

Тема 3.1 Цифровой профиль: безопасность социальных сетей **(4 часа).**

Теория: Изучение психологических аспектов взаимодействия человека с интернетом. Цифровой профиль современного интернет-пользователя. Поисковые системы и основы работы с браузерами. Разбор безопасности современных социальных сетей и мессенджеров.

Практика: Работа с браузерами и расширениями. Изучение страничек профиля в ВК и Одноклассники. Телеграмм и его особенности.

Тема 3.2 Общение в сети **(2 часа).**

Теория: Изучение основных принципов эффективного общения в онлайн-среде. Нормативно-правовые акты, регулирующие информационное взаимодействие в России. Ознакомление с основными принципами безопасного общения в интернете, включая защиту личной информации, предотвращение кибербуллинга и обмана, а также умение распознавать и избегать потенциально опасных ситуаций.

Практика: Интерактивная игра по теме «Общение в сети».

Тема 3.3 Поиск информации в сети **(6 часов).**

Теория: Что такое поисковые системы, их роль в Интернете, и как они работают. Как формулировать эффективные запросы для получения нужной информации. Оценка достоверности информации.

Практика: Выполнение задания по поиску различной информации в сети. Использование сервиса поиска людей в Интернете.

Текущий контроль по разделу «Цифровое пространство» (**1 час**, Приложение 2).

Раздел 4. Взлом и его последствия (9 часов).

Тема 4.1 Мошенничество **(4 часа).**

Теория: Взлом и его последствия для современного пользователя. Что может пострадать при взломе. Виды мошенничества и угроз. Виды злоумышленников. Архивы.

Практика: Интерактивная игра «Кто предатель». Разбор реальных примеров мошенничества и путей борьбы с ним. Работа с архивами.

Тема 4.2 Пароли и шифрование **(2 часа).**

Теория: Виды паролей, менеджеры паролей. Шифрование, генерация паролей. Шифр Цезаря, шифр Виженера. Многофакторная аутентификация.

Практика: Работа с шифрами и паролями.

Тема 4.3 Вирусы и вредоносное ПО **(2 часа).**

Теория: Виды вирусов. Самые страшные вредоносные ПО в истории человечества. Обучение методам защиты от вирусов и вредоносного ПО. Антивирусные системы.

Практика: Рассмотрение в реальном времени как вирусное ПО уничтожает систему. Правила работы с антивирусными системами.

Текущий контроль по разделу «Взлом и его последствия» (**1 час**, Приложение 3).

Раздел 5. Нейросети и искусственный интеллект (21 час).

Тема 5.1 Введение в нейросети и ИИ **(4 часа).**

Теория: Понятие ИИ и нейросетей, история развития, примеры использования.

Практика: Демонстрация простых инструментов ИИ.

Тема 5.2 Промпт-инжиниринг: как задавать вопросы нейросетям **(4 часа).**

Теория: Принципы правильной постановки задач для ИИ.

Практика: Составление промптов и анализ качества ответов работы ИИ.

Тема 5.3 Применение ИИ в учёбе и проектах **(10 часов).**

Теория: Обзор инструментов генерации текста, изображений, видео и музыки.

Практика: Выполнение заданий – создание иллюстраций, подготовка реферата, генерация идей для проектов.

Тема 5.4 Культура использования ИИ: этика, правовые и социальные аспекты **(2 часа).**

Теория: Законодательство об ИИ, авторское право, ответственность за использование ИИ.

Текущий контроль по разделу «Нейросети и искусственный интеллект» **(1 час).**

Раздел 6. Разработка и защита итогового проекта (7 часов).

Тема 6.1 Создание своей памятки по кибергигиене и нейросетям **(5 часов).**

План работы:

1. Определиться с темой итогового проекта.
2. Определиться с формой оформления итогового проекта.
3. Реализация оформления проекта (презентация, бумажная памятка, графическая работа, видеоролик).
4. Подготовка к защите итогового проекта.

Тема 6.2 Защита проектов **(2 часа).**

Выступление с итоговым проектом, ответ на вопросы и подведение итогов программы.

4. СПИСОК ЛИТЕРАТУРЫ

1. Ашманов Игорь Станиславович; Касперская Наталья Ивановна. "Цифровая гигиена." Издательство Питер, 2022.
2. Ковалев Андрей. "Основы кибергигиены: практическое руководство." Издательство "Цифровая безопасность", Санкт-Петербург, 2019.
3. Ефимова, Л.Л. "Информационная безопасность детей. Российский и зарубежный опыт." / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2016.
4. Федотова Г. В. "Угрозы кибербезопасности устойчивости цифровых платформ." Екатеринбург, 2021.
5. Иванов Дмитрий. "Основы информационной безопасности." Издательство "ИнфоБез", Москва, 2017.
6. Сидорова Елена. "Практическое руководство по обеспечению информационной безопасности." Издательство "ИнформБез", Санкт-Петербург, 2020.
7. Петров, С.В. "Информационная безопасность: Учебное пособие" / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2016.
8. Ярочкин, В.И. "Информационная безопасность: Учебник для вузов" / В.И. Ярочкин. — М.: Акад. Проект, 2018.
9. Гладков А. Н. "Визуализация киберугроз как аспект формирования компетенций в области информационной безопасности" / А. Н. Гладков, С. Н. Горячев, Н. С. Кобяков // Защита информации. Инсайд. - 2023.
10. Кузьмина О. В. "Информационно-технологическая безопасность обучающихся. " Екатеринбург, 2021.
11. Гудфеллоу И., Бенджио Й., Курвилль А. Глубокое обучение. — М.: ДМК Пресс, 2017.
12. Рассел С., Норвиг П. Искусственный интеллект: современный подход. — М.: Вильямс, 2020.
13. Кулешов А. Нейросети. Полный курс. — СПб.: Питер, 2021.
14. Чжан К., Лью Г. Практика работы с ChatGPT и промпт-инжиниринг. — М.: Эксмо, 2023.

5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Материально – техническое обеспечение:

1. Стол преподавателя
2. Стул преподавателя
3. Стол обучающегося
4. Стул обучающегося
5. Рабочая станция преподавателя
6. Ноутбук обучающегося
7. Интерактивная доска
8. Проектор
9. МФУ
10. Точки подключения к электрической сети

Программное обеспечение:

1. Операционная система Windows 10
2. Пакет программ MS OFFICE

Приложение 1

Тест по разделу «Основы кибергигиены».

ФИО_____

Вопрос 1. Что такое кибергигиена?

А) Защита компьютеров от вредоносных программ.

Б) Правила безопасного поведения в интернете.

В) Процесс создания новых технологий.

Вопрос 2. Что такое информационная безопасность?

А) Защита информации от несанкционированного доступа и разрушения.

Б) Способность компьютера быстро обрабатывать информацию.

В) Процесс разработки новых методов шифрования.

Вопрос 3. Какие меры безопасности важно соблюдать в сети Интернет?

А) Никому не сообщать личные данные и пароли.

Б) Регулярно обновлять антивирусное ПО.

В) Использовать один и тот же пароль для всех аккаунтов.

Вопрос 4. Кто такие ИБ-специалисты?

А) Люди, ответственные за ведение социальных сетей.

Б) Специалисты по информационной безопасности, обеспечивающие защиту данных.

В) Инженеры, разрабатывающие новые программы для интернета.

Вопрос 5. Что такое фактчекинг?

А) Проверка достоверности информации с целью определения ее правдивости.

Б) Процесс создания фотографий и видеороликов для социальных сетей.

В) Использование фильтров для обработки изображений.

Ответы: б) а) а) б) а).

Вопрос 6 (в форме билетов):

1 Билет (Word)

Создать в текстовом редакторе Word документ по предлагаемому образцу, используя:

- различные подходящие типы автофигур;
- оформление автофигур при помощи тени;
- различные типы и цвета линий и цвета заливки.

СХЕМА ФИНАНСОВЫХ ПОТОКОВ ПРЕДПРИЯТИЯ



2 Билет (Word)

Верхний колонтитул заполните следующим текстом: Александр Пушкин «Ты и Вы». Наберите текст стихотворения:

Ты и Вы

Пустое вы сердечным ты

Она, обмолвясь, заменила

И все счастливые мечты

В душе влюбленной возбудила.

Пред ней задумчиво стою,

Свести очей с нее нет силы;

И говорю ей: как вы милы!

И мыслю: как тебя люблю!

Выполните команду со шрифтом:

- **для заголовка**: шрифт – Century Gothic, начертание – полужирный, размер – 18 пт, цвет – красный, интервал между символами – разреженный 6 пт;
- **для остального текста**: шрифт – Tahoma, размер – 14 пт, цвет – фиолетовый, видоизменение – с тенью.

3 Билет (Word)

Верхний колонтитул заполните следующим текстом: Александр Пушкин «Ты и Вы». Наберите текст стихотворения:

Ты и Вы

Пустое вы сердечным ты

Она, обмолвясь, заменила

И все счастливые мечты

В душе влюбленной возбудила.

Пред ней задумчиво стою,

Свести очей с нее нет силы;

И говорю ей: как вы милы!

И мыслю: как тебя люблю!

Выполните команду с абзацем:

- **для заголовка**: выравнивание – по центру, интервал перед абзацем – 6 пт, после абзаца – 6пт;
- **для остального текста**: выравнивание – по левому краю, отступ слева – 3 см, интервал после абзаца – 6 пт, междустрочный интервал – одинарный.

4 Билет (Word)

Создайте следующий многоуровневый список:

Устройства современного компьютера
1. Процессор
2. Память
    2.1. Оперативная память
    2.2. Долговременная память
        2.2.1. Жесткий магнитный диск
        2.2.2. Дискета
        2.2.3. Флэш-память
        2.2.4. Оптические диски
            2.2.4.1. CD
            2.2.4.2. DVD
3. Устройства ввода
    3.1. Клавиатура
    3.2. Мышь
    3.3. Сканер
    3.4. Графический планшет
    3.5. Цифровая камера
    3.6. Микрофон
    3.7. Джойстик
4. Устройства вывода
    4.1. Монитор
        4.1.1. Жидкокристаллический монитор
        4.1.2. Монитор на электронно-лучевой трубке
    4.2. Принтер
        4.2.1. Матричный принтер
        4.2.2. Струйный принтер
        4.2.3. Лазерный принтер

5 Билет (Word)

Создайте следующую таблицу:

№	Название маршрута (пункт отправления – конечный пункт)	Время		Цена билета, руб	Количество проданных билетов, шт	Общая стоимость, руб
		отправления	прибытия			
Итого:						

Ввести произвольные данные и используя формулу СУММА, вычислить итоговую строку.

Вопрос 7 (в форме билетов):

6 Билет (Exel)

10 студентов сдают экзамены по 5 дисциплинам. По каждой дисциплине можно получить оценку – 2, 3, 4, 5. Определить среди 10 студентов человека с наибольшим средним баллом. Построить диаграмму, показывающую соотношение оценок, полученных каждым студентом по каждой дисциплине.

7 Билет (Exel)

10 спортсменов принимают участие в некотором соревновании. Каждый спортсмен может набрать не более 30 очков. Указать номер места, которое занял спортсмен в данном соревновании. За 1 место выплачивается премия 100000 руб., за 2 место 50000 руб. и за 3 место 30000 руб. Построить диаграмму, показывающую количество набранных очков, каждым спортсменом.

8 Билет (Exel)

Ввести информацию в таблицу по образцу. Выполнить соответствующие вычисления (использовать абсолютную ссылку для курса доллара). Построить сравнительную круговую диаграмму цен на товары. Диаграммы красиво оформить, сделать заголовки и подписи к данным.

Расчет стоимости проданного товара

Товар	Цена в дол.	Цена в рублях	Количество	Стоимость
Шампунь	$4,00			
Набор для душа	$5,00			
Дезодорант	$2,00			
Зубная паста	$1,70			
Мыло	$0,40			
Курс доллара.				

Стоимость покупки	

9 Билет (Exel)

Построить на промежутке [-2, 2] с шагом 0,4 таблицу значений функции:

$$y = \begin{cases} \cos(3x^2) & при\ x \le 0, \\ \sqrt{0{,}5x} & при\ x \ge 0 \end{cases}$$

10 Билет (Exel)

Составьте ведомость контроля остаточных знаний студентов по какой-либо дисциплине. Контроль остаточных знаний проходит в форме теста, по результатам которого выставляется оценка. Если студент набрал от 95 до 100 баллов, выставляется оценка «5», от 80 до 94 – «4», от 60 до 79 – «3», менее 60 – «2». Посчитайте: количество студентов, получивших оценку «5», «4», «3», «2», средний балл в группе, максимальный и минимальный баллы. С помощью диалогового окна Условное форматирование выделите все «2» красным цветом. Постройте круговую диаграмму, показывающую процентное соотношение оценок в группе.

Приложение 2

Тест по разделу «Основы кибергигиены».

ФИО_____

Вопрос 1. Что такое цифровой профиль интернет-пользователя?

А) Это уникальный номер пользователя, используемый для аутентификации в сети.

Б) Это совокупность информации о пользователе в цифровой форме, которая хранится и обрабатывается в сети Интернет.

В) Это секретные данные о пользователе, предоставляемые только владельцу устройства.

Вопрос 2. Какие основные функции выполняют поисковые системы в интернете?

А) Сохранение файлов на серверах и передача данных между пользователями.

Б) Изучение и анализирование информации, сбор данных о веб-страницах и формирование релевантных результатов поиска.

В) Предоставление доступа к социальным сетям и мессенджерам.

Вопрос 3. Что такое кибербуллинг?

А) Это методика защиты компьютерных систем от вирусов и хакерских атак.

Б) Это форма электронного домогательства, осуществляемая через интернет, с использованием различных онлайн-платформ.

В) Это термин, описывающий процесс поиска информации в интернете с использованием поисковых систем.

Вопрос 4. Какие нормативно-правовые акты регулируют информационное взаимодействие в России?

А) Конституция Российской Федерации и Федеральный закон "О связи".

Б) Кодекс Российской Федерации об административных правонарушениях и Налоговый кодекс Российской Федерации.

В) Устав города Москвы и Правила дорожного движения.

Вопрос 5. Какие основные принципы эффективного общения в онлайн-среде вы знаете?

А) Использование агрессивного языка и предъявление претензий к собеседнику.

Б) Соблюдение правил этикета и вежливость в общении, уважение к мнению других и толерантность.

В) Использование грубых и непристойных выражений, чтобы привлечь внимание к своим сообщениям.

Приложение 3

Тест по разделу «Взлом и его последствия».

ФИО_____

Вопрос 1. Что такое взлом компьютерной системы, и какие могут быть его последствия?

Вопрос 2. Какие виды вирусов вы знаете?

Вопрос 3. Какие вредоносные программы считаются самыми страшными в истории человечества?

Вопрос 4. Какие методы защиты от вирусов и вредоносного ПО вы можете предложить?

Вопрос 5. Что такое многофакторная аутентификация?

Вопрос 6. Что такое шифрование, и зачем оно используется?

Вопрос 7. Посмотрите на картинку. Под какими номерами находятся ненадёжные пароли?

1) 1234
2) 1111
3) Uy784fg*fgdgd///dfg
4) Df56rrr*/ghgd
5) Qwerty
6) 5544
7) Fg-*/h525&413%

Вопрос 8. Будет ли надёжным пароль, если использовать в нём слова, в которых используются очевидные замены букв специальными символами (например, h0use - замена буквы о на цифру ноль)?

Вопрос 9. Зашифрованное: н л е з у д л д л з р г, со сдвигом 3. Необходимо расшифровать слово.