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

РЕКОМЕНДОВАНО:
Председатель методического совета
_____Н.В. Грицюк
протокол № 12
от «3» апреля 2024 г.

УТВЕРЖДАЮ:
Директор филиала
_____Е.А. Дыптан
Приказ № 02-02-59
от «3» апреля 2024 г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

технической направленности

«Кибергигиена и работа с большими данными»

Срок реализации: 72 часа (1 год)
Возраст детей: 15-17 лет
Составитель программы:
Шикан А.В., педагог дополнительного образования

г. Норильск, 2024 г.

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная общеобразовательная общеразвивающая программа «Кибергигиена и работа с большими данными» имеет техническую направленность и разработана 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.

Человечество входит в пору четвёртой промышленной революции, которая кардинально изменит образ жизни человека: систему ценностей, критерии важности, принципы взаимоотношений в обществе. Информация становится доступнее, и, как следствие, образование и самообразование, а также способы самореализации выходят на качественно иной уровень.

Основная среда для использования цифровых технологий — глобальная сеть. При этом современные технологии размывают границы использования цифровой техники в рамках Сети или локально до такой степени, что большинство пользователей даже не задумывается о том, что использует Интернет. Интернет из академического мира шагнул сначала в каждый дом, а дальше стал постоянным спутником человека без привязки к конкретному месту и в любой момент времени.

Снижение цен на электронные устройства и на тарифы доступа к Интернету, развитие мобильного интернета и высокоскоростных линий передачи данных являются катализаторами этого процесса. В России пользователей Интернета на данный момент более 80% населения. И с каждым годом эта цифра увеличивается. При этом пользователями Интернета являются не только взрослые.

Как показывают различные исследования, дети начинают пользоваться Интернетом уже в возрасте 6-8 лет. Становится очевидным, что учиться жить в новых реалиях — необходимость, а бурное развитие цифровых технологий обуславливает потребность наличия соответствующих образовательных материалов, затрагивающих все аспекты их применения.

Умение использовать цифровые технологии, и Интернет, в частности, нашло свое отражение в виде включения данного умения в Федеральный государственный стандарт общего образования. Но в рамках школьной программы достаточно сложно подробно осветить все аспекты современной цифровой жизни общества, что обуславливает необходимость отдельного курса, посвящённого этим вопросам.

1.1. НОВИЗНА ДООП

Программа «Кибергигиена и работа с большими данными» в целом строится на концепции подготовки учащихся к профессии киберследователя, проектировщика личной безопасности, цифрового лингвиста – профессиям будущего, выделенным в «Атласе новых профессий» (проект «Агентства стратегических инициатив» по исследованию рынка труда, 2015 г.) и предполагающим проведение расследований киберпреступлений посредством поиска и обработки информации в интернет-пространстве.

1.2. АКТУАЛЬНОСТЬ ДООП

Кибергигиена и кибербезопасность становятся все более важными в современном мире в связи с растущими угрозами, такими как хакерские атаки, вирусы и другие виды киберпреступности. Эти угрозы становятся сложными и разнообразными, поэтому в наше время как среди взрослого населения, так и среди детей растет осознание важности базовых навыков безопасности. Это, в свою очередь, приводит к совершенствованию методов защиты информации и компьютерных систем. Развитие технологий также приводит к возрастанию уровня цифровой уязвимости, что подчеркивает важность соблюдения мер кибергигиены и принятия эффективных мер по обеспечению кибербезопасности. С увеличением случаев использования интернета и цифровых устройств становится важным обучать школьников правилам безопасного поведения в сети, защите своих личных данных и предотвращению киберугроз. Понимание основных принципов кибербезопасности поможет школьникам избегать опасных ситуаций в онлайн-среде и развивать ответственное поведение в интернете. Понимание основ анализа больших данных поможет им развить навыки работы с информацией, критического мышления и принятия обоснованных решений на основе фактических данных. Эти навыки могут быть полезны как в учебе, так и в будущей профессиональной деятельности. Кроме того, изучение больших данных может подготовить школьников к будущим технологическим трендам и помочь им лучше понять роль данных в современном обществе. Эта программа помогает подготовить учащихся к вызовам современного информационного мира.

1.3. ПЕДАГОГИЧЕСКАЯ ЦЕЛЕСООБРАЗНОСТЬ

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.

Программа фокусируется 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 попробуют себя в роли киберпреступников для лучшего понимания уязвимых сторон современного информационного пространства. Программа направлена на создание благоприятной обстановки для личностного роста обучающихся, их успешную социализацию, так как большая часть занятий направлена на общение обучающихся и работу в командах. Таким образом, курс представляет из себя не череду монотонных лекций, а работу со школьниками в интерактивном формате, для повышения эффективности изучения ребятами сложных тем, будут использоваться медиа материалы собственного производства.

Программа ориентирована на развитие технических и творческих способностей обучающихся, формирование знаний, умений, и навыков в области визуализации и анализа данных базового уровня, организацию исследовательской и проектной деятельности, а также овладение универсальными навыками, не связанными с конкретной предметной областью, такими как взаимопомощь, организаторские и лидерские качества, аккуратность, самостоятельность, ответственность, дисциплинированность.

1.4. ЦЕЛЬ ДООП

Целью ДООП является формирование у обучающихся компетенций, дающих возможность комплексно анализировать получаемую информацию, размещенную в сети Интернет, обучение правилам безопасного поведения в цифровом пространстве, эффективному использованию интернета и цифровых технологий в повседневной жизни.

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.

1.5. ВОЗРАСТ ОБУЧАЮЩИХСЯ, УЧАСТВУЮЩИХ В ДООП

Программа «Кибергигиена и работа с большими данными» рассчитана на обучающихся 15-17 лет. Максимальное количество обучающихся в группе – 12 человек.

1.6. УСЛОВИЯ ВХОЖДЕНИЯ В ДООП

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, должны иметь базовые навыки использования ПК, пакета Microsoft Office, начальный уровень знания английского языка.

1.7. СРОК РЕАЛИЗАЦИИ ДООП

Программа рассчитана на 72 учебных часа. Срок освоения программы – 1 год.

1.8. РЕЖИМ ЗАНЯТИЙ, ФОРМЫ И МЕТОДЫ ОБУЧЕНИЯ

Учебные занятия проходят в очной форме. Режим занятий – 1 раз в неделю по 2 академических часа (1 академический час - 40 минут) с обязательным перерывом.

Форма обучения – очная.

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.

1.9. ОЖИДАЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ И ЭФФЕКТЫ, СПОСОБЫ ПРЕДЪЯВЛЕНИЯ И ОТСЛЕЖИВАНИЯ РЕЗУЛЬТАТОВ

Результаты освоения программы «Кибергигиена и работа с большими данными»:

- наличие знаний о базовых принципах безопасного поведения в сети, включая защиту личной информации, использование надежных паролей и определение подозрительных ситуаций;
- сформированы навыки собора, обработки и анализа больших объемов данных, обучающийся умеет выявлять в них закономерности и тренды, а также делать выводы на основе полученной информации;
- получены навыки использования современных методов защиты информации, включая шифрование, аутентификацию, межсетевые экраны и прочие средства обеспечения безопасности;
- изучены этические и правовые нормы, касающиеся использования данных и информации в сети;
- развиты навыки коммуникации и сотрудничества в коллективе, необходимые для эффективной работы в области информационной безопасности и будущей профессиональной деятельности;
- приобретены навыки самостоятельной организации своей деятельности таким образом, чтобы сформировать основу для дальнейшего саморазвития и самовоспитания.

Во время занятий текущий контроль освоения программы осуществляется через наблюдения, опросы и тестирования. Обучение разделено на несколько основных тем, по окончанию изучения которых обучающимся будут выдаваться контрольные работы в виде теста. Итоговая аттестация происходит путем презентации финальной работы (проекта), которая заключается в создании собственной памятки по пройденным темам курса (бумажная памятка, видео-урок и тд.) и 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	2	0	
Раздел 2. Основы кибергигиены (16 часов)					
2.1	Знакомство с основами безопасности.	2	1	1	
2.2	Фактчекинг. Зачем нам знать ложь изнутри?	2	1	1	
2.3	Основы компьютерной грамотности.	11	4	7	
2.4	Текущий контроль по разделу «Основы кибергигиены».	1	0	1	Фронтальный опрос, тестирование.
Раздел 3. Цифровое пространство (19 часов)					
3.1	Цифровой профиль: безопасность социальных сетей.	8	4	4	
3.2	Общение в сети.	4	2	2	
3.3	Поиск информации в сети.	6	2	4	
3.4	Текущий контроль по разделу «Цифровое пространство».	1	0	1	Фронтальный опрос, тестирование.
Раздел 4. Взлом и его последствия (15 часов)					
4.1	Мошенничество.	6	2	4	
4.2	Пароли и шифрование.	4	2	2	
4.3	Вирусы и вредоносное ПО.	4	2	2	
4.4	Текущий контроль по разделу «Взлом и его последствия».	1	0	1	Фронтальный опрос, тестирование.
Раздел 5. Работа с большими данными (12 часов)					
5.1	Введение в большие данные	4	2	2	
5.2	Визуализация данных	6	2	4	
5.3	Культура работы с данными	2	1	1	
Раздел 6. Разработка и защита итогового проекта (6 часов)					

6.1	Создание своей памятки по кибергигиене.	4	0	4	
6.2	Защита проектов.	2	0	2	Теоретическое тестирование, защита проекта.
	ИТОГО	72	26	46	

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 инструментов. Правила пожарной безопасности. Процедуры действий в случае аварийных ситуаций или чрезвычайных ситуаций. Требования к чистоте и порядку на рабочем месте, включая уборку и утилизацию отходов.

Раздел 2. Основы кибергигиены (16 часа)

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 Основы компьютерной грамотности **(11 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» (**1 час**, Приложение 1).

Раздел 3. Цифровое пространство (19 часов).

Тема 3.1 Цифровой профиль: безопасность социальных сетей **(8 часов).**

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 **(4 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 (15 часов).

Тема 4.1 Мошенничество **(6 часов).**

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 **(4 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 **(4 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. Работа с большими данными (12 часов).

Тема 5.1 Введение в большие данные **(4 часа).**

Теория: Понятие данных и как с ними работать. Жизненный цикл данных. Технологии сбора больших данных.

Практика: Сбор и анализ данных из интернета (Яндекс Аналитика). Использование онлайн-инструментов для анализа данных, создание собственной формы, для дальнейшего изучения полученных данных.

Тема 5.2 Визуализация данных **(6 часов).**

Теория: Основные способы и подходы визуализации данных. Требования и рекомендации к визуализации данных.

Практика: Использование онлайн-инструментов для анализа данных, построение графиков и диаграмм и их визуальное оформление.

Тема 5.3 Культура работы с данными **(2 часа).**

Теория: Значение данных. Ответственность за данные. Культура обмена данных.

Практика: Тестирование по теме (Приложение 4).

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

Тема 6.1 Создание своей памятки по кибергигиене **(4 часа).**

План работы:

1. Определиться с темой итогового проекта.
2. Определиться с типом оформления итогового проекта.
3. Реализовать оформление проекта (презентация, бумажная памятка, графическая работа, видеоролик).
4. Подготовиться 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.

5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ 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

6. МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ПО РАЗДЕЛАМ ПРОГРАММЫ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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).

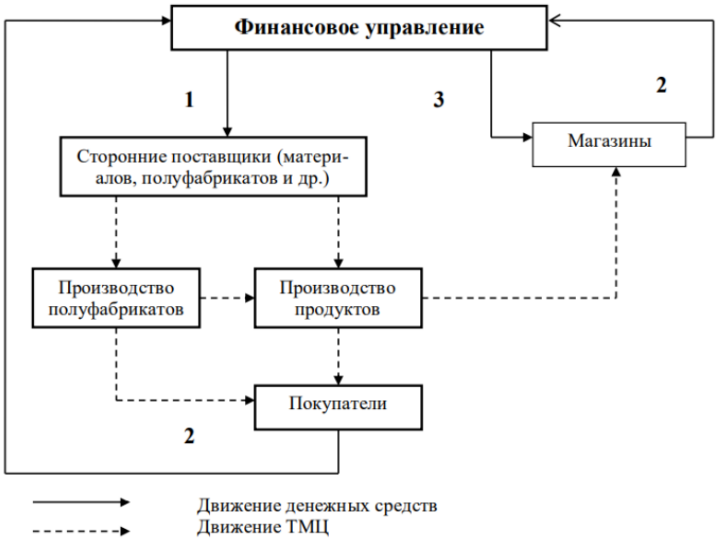
Вопрос 6 (в форме билетов):

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.

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.

7 Билет (Exel)

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?

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.