МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБРАЗОВАНИЕ НАЦИОНАЛЬНЫЕ ПРОЕКТЫ РОССИИ

СЕТЬ ЦЕНТРОВ ЦИФРОВОГО ОБРАЗОВАНИЯ ДЕТЕЙ «IT-КУБ»

РАССМОТРЕНО
на заседании педагогического совета
протокол от 28.08.2023 г. № 1

УТВЕРЖДАЮ
директор МБОУ СОШ № 14
приказ от 28.08.2023 г. № 94/4

Дополнительная общеобразовательная программа «Кибергигиена. Мир социальных медиа» по тематическому направлению «Кибергигиена и работа с большими данными» с использованием оборудования центра цифрового образования детей «IT-куб»

Направленность:
техническая
Возраст: 11-18 лет

г.Новошахтинск
2023 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Интернет – всемирная система объединенных компьютерных сетей для хранения и передачи информации, которая, главным образом, предназначалась для использования правительством и государственными органами, а позже для исследовательских и образовательных сообществ. В настоящее время без сети Интернет невозможно представить свою жизнь, он проник во все сферы нашей жизни и выполняет множество функций, такие как информационная, коммуникативная, образовательная и т. д. Многие люди не могут представить себе жизнь без глобальной сети, особенно без социальных сетей. Страница человека в социальной сети - виртуальное лицо современного человека, поэтому очень важно уметь ориентироваться в огромном объеме информации, отличать достоверную информацию от ложной, обезопасить себя и свои личные данные от негативных действий других пользователей сети.

Направленность программы

Программа носит междисциплинарный характер и позволяет решить задачи развития у учащихся научно-исследовательских, технико-технологических и гуманитарных компетенций.

Актуальность программы

Программа знакомит учащихся с методическими основами и практикой анализа информации в интернет-пространстве и демонстрирует социальную значимость аналитической работы.

В ходе освоения программы, учащиеся получат навыки исследовательской деятельности и анализа информации в интернет-пространстве, смогут обнаруживать источники информации, каналы и способы ее распространения. Также учащиеся научатся распознавать опасный и вредоносный контент, манипулирование сознанием и внушение потенциально опасных идей в интернет-пространстве. Полученные знания и умения позволят критически оценивать и классифицировать получаемую в интернет-пространстве информацию, использовать ее в положительных целях и нейтрализовать ее негативное влияние.

Новизна программы

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

Целью программы является развитие творческих способностей учащихся к комплексному анализу информации, размещенной на различных интернет-ресурсах, в интересах безопасного и рационального использования интернет-пространства, формирование информационной культуры.

Реализация цели программы осуществляется через определенные **задачи:**

Образовательные:

- сформировать у учащихся представление о структуре и типах информации в интернет-пространстве, больших данных и больших пользовательских данных;
- ознакомить учащихся с методами и средствами поиска информации в интернет-пространстве;
- сформировать у учащихся способность распознавать опасный и вредоносный контент и идентифицировать явления манипулирования сознанием в интернет-пространстве, внушения деструктивных идей и вовлечения в социально опасные группы в социальных сетях;

сформировать у учащихся способность определять социальные характеристики и

индивидуальные особенности людей и обнаруживать признаки опасного поведения на основании

- обучить учащихся приемам противодействия негативным воздействиям в интернет-пространстве.

Воспитательные:

- сформировать у учащихся культуру позитивного использования интернет-пространства;
- в защищенной среде продемонстрировать учащимся возможные угрозы и риски интернет-пространства;
- привить информационную культуру: ответственное отношение к информации с учетом правовых и этических аспектов её распространения, избирательного отношения к полученной информации.

Развивающие:

- ознакомить учащихся с основами исследовательской деятельности (принципами построения исследования, процедурой и этикой его проведения, количественными и качественными методами обработки полученных данных);
- сформировать у учащихся способность выявлять и критически оценивать источники и каналы распространения информации в интернет- пространстве и определять ее качество;
- сформировать у учащихся способность успешной самопрезентации и создания позитивного имиджа в социальных сетях;
- сформировать у учащихся навыки планирования, проведения и обработки результатов исследования информации в интернет-пространстве при помощи поисковых систем, общедоступных средств поиска информации и системы мониторинга и анализа социальных медиа «Крибрум»;
- развивать познавательные способности ребенка, память, внимание, пространственное мышление, аккуратность и изобретательность.

Отличительные особенности программы

Программа направлена на формирование у учащихся базовых компетенций в области исследовательской деятельности в целом и анализа информации в интернет-пространстве в частности. Она акцентирует внимание на медиаграмотности и анализе информации в интернет-пространстве в контексте психологической безопасности личности. Особое внимание уделяется социальным сетям. Также будет рассмотрена технология «big data», которая позволяет работать со структурированными и неструктурированными данными огромных объемов и содержания, а также будут изучены методы их обработки, которые позволяют анализировать информацию.

Условия реализации программы.

Возраст обучающихся, участвующих в реализации программы: 14 - 17 лет.

На курс программы зачисляются все желающие при наличии свободных мест. Программа предназначена для детей, проявляющих интерес к информационным технологиям, стремящихся к саморазвитию, профессиональному самоопределению.

Программа является общеразвивающей (базовый уровень), не требует предварительных знаний и входного тестирования.

Сроки реализации: общая продолжительность программы – 68 часов.

Режим занятий: два часа один раз в неделю.

Форма реализации программы — смешанная / очная с использованием электронногообучения.

Под электронным образованием понимается реализация образовательных программ сиспользованием информационно - образовательных ресурсов, информационно-коммуникационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу информационно-образовательных ресурсов и взаимодействие участников образовательного пространства.

Формы организации деятельности обучающихся

При изучении тем программа предусматривает использование фронтальной, индивидуальной и групповой формы учебной работы обучающихся, в том числе:

- интерактивные лекции;
- практическая работа;
- самостоятельная работа учащихся (индивидуально и в малых группах);
- конференции.

Приветствуются встречи с приглашенными спикерами, совместные конференции, видеоконференции или вебинары с экспертами, индивидуальные и групповые консультации

Содержание курса:

Данный курс состоит из вводного кейса и 8 основных кейсов.

Вводный кейс. Настройки безопасности персонального компьютера. Порядок действий ликвидации последствий сбоев системы.

1. Основы анализа информации в интернет-пространстве.

2. Угрозы в интернет-пространстве, методы противодействия.

3. Основы работы в социальных сетях.

4. Безопасное и рациональное использование личных и персональныхданных в социальных сетях.

5. Распознавание опасного и вредоносного контента в интернет-пространстве.

6. Безопасность мобильных устройств.

7. Угрозы безопасности в сетях WiFi. Онлайн сервисы безопасности.

8. Обработка и анализ больших данных. Основные принципы построения нейросетей.

.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН «КИБЕРГИГИЕНА И РАБОТА С БОЛЬШИМИ ДАННЫМИ»

№	Наименование кейса, темы	Количество часов		
		Теория	**Практика**	**Всего**
	Вводны кейс. Настройки безопасности персонального компьютера. Порядок действий ликвидации последствий сбоевсистемы.	**3**	**3**	**6**
1.	Тема 1. Разграничение правпользователей.	1	1	2
2.	Тема 2. Понятие сбоя системы и синего экрана. Способы восстановления системы. Изучение сообщений о синем экране с помощью системы «Крибрум».	1	1	2
3.	Тема 3. Брендмауэры и фаерволы. Работа в браузере. Настройки безопасности.	1	1	2
	Кейс 1. Основы анализа информации в интернет-пространстве.	**2**	**2**	**4**
4.	Тема 1.1 Информационная структураинтернета, поисковые системы.	0,5	0,5	1
5.	Тема 1.2. Принципы эффективного поиска информациив интернете. Принципы оценки качества источников информации.	0,5	0,5	1

6.	Тема 1.3. Определение больших данных. Технологии хранения больших данных.	1	1	2
	Кейс 2. Угрозы в интернет-пространстве, методы противодействия.	**5**	**5**	**10**
7.	Тема 2.1. Вирусные атаки ПК. Классы вирусов, способы защиты. Изучение сообщений о вирусных атаках с помощью системы «Крибрум».	1	1	2
8.	Тема 2.2. Антивирусные программы. Методология выбора оптимальной антивирусной программы для личного ПК.	1	1	2
9.	Тема 2.3. Фейковые сообщения ивредоносное ПО в сети Интернет.	1	1	2
10.	Тема 2.4. Хакерские атаки, виды атак. Исследование юридических аспектов проблемы хакерства с помощью поисковых систем.	1	1	2
11.	Тема 2.5. Проблема кражперсональных данных с помощью вредоносного ПО.	0,5	0,5	1
12.	Тема 2.6. Проблема краж с помощьюбанковских карт.	0,5	0,5	1
	Кейс 3. Основы работы всоциальных сетях.	**2**	**2**	**4**
13.	Тема 3.1. Социальные сети исоциальные медиа.	0,5	0,5	1
14.	Тема 3.2. Поведение молодежи в сети,проблема лайков.	0,5	0,5	1
15.	Тема 3.3. Понятие социальная группа, сообщество, субкультура. Правила функционирования сетевых сообществ. Правила сетевого общения. Анализ сообществ спомощью системы «Крибрум».	1	1	2
	Кейс 4. Безопасное и рациональноеиспользование личных и персональных данных в социальных сетях.	**3**	**3**	**6**
16.	Тема 4.1. Защищенность данных в сети.Проблемы утечки данных.	0,5	0,5	1
17.	Тема 4.2. Создание безопасных паролей.	0,5	0,5	1
18.	Тема 4.3. Социальные сети: пользовательские соглашения, права и обязанности.	0,5	0,5	1
19.	Тема 4.4. Структура аккаунта пользователя социальной сети.Самопрезентация пользователя всоциальных сетях. Проблема репостов,юридический аспект.	0,5	0,5	1
20.	Тема 4.5. Проблемы использования всообщениях геотегов.	0,5	0,5	1
21.	Тема 4.6. Исследование аккаунтов в социальных сетях с использованием контент-анализа, анализ личных профилей в социальных сетях.	0,5	0,5	1
	Кейс 5. Распознавание опасногои вредного контента в интернет-пространстве.	**10**	**10**	**20**
22.	Тема 5.1. Проблема контентных рисковии меры противодействия им.	1	1	2
23.	Тема 5.2. Правила противодействия фишингу. Исследование фишинговых и коротких ссылок с помощью системы «Крибрум».	1	1	2
24.	Тема 5.3. Интернет-коммерция. Площадки для Интернет-торговли. Проверка подлинности интернет-магазина.	1	1	2

25.	Тема 5.4. Благотворительность спомощью интернет.	1	1	2
26.	Тема 5.5. Риски потребительского поведения. Объявления о дарении, конкурсы репостов.	0,5	0,5	1
27.	Тема 5.6. Проблема оказания поддельных услуг и распространения подозрительных объявлений об удаленной работе в социальных сетях.	0,5	0,5	1
28.	Тема 5.7. Правила социальных сетей поразмещению рекламы.	0,5	0,5	1
29.	Тема 5.8. Сетевые игры: польза и вред. (Сетевые игры как массовые развлечения. Бесплатные и платные игры. Для чего может быть полезен ПК и Интернет и как польза превращается во вред.)	0,5	0,5	1
30.	Тема 5.9. Киберугрозы Интернета. Кибертерроризм и кибервойны.	0,5	0,5	1
31.	Тема 5.10. Кибершпионаж.Кибероружие.	0,5	0,5	1
32.	Тема 5.11. Борьба с использованием Интернета в террористических, сепаратистских и экстремистских целях. Интернет как оружие массовогопоражения.	1	1	2
33.	Тема 5.12. Понятие интернет- зависимости, компьютерной зависимости и причин их возникновения.Интернет-сообщество. Зависимость от интернет-общения. Виртуальнаяличность.	1	1	2
34.	Тема 5.13. Развлечения в Интернет.Признаки зависимости. Сайтызнакомств. Управление личностьючерез сеть. Киберкультура и личность. Типы интернет-зависимости.	1	1	2
	Кейс 6. Безопасность мобильныхустройств.	**2**	**2**	**4**
35.	Тема 6.1. Безопасность мобильных устройств в информационных системах.	0,5	0,5	1
36.	Тема 6.2. Источники заражениямобильных устройств.	0,5	0,5	1
37.	Тема 6.3. Угрозы для IOS-устройств.Угрозы для Android-устройств.	0,5	0,5	1
38.	Тема 6.4. Рост числа угроз для мобильных устройств. Вирусы для мобильных устройств.	0,5	0,5	1
	Кейс 7. Угрозы безопасности в сетяхWiFi. Онлайн сервисы безопасности.	**3**	**3**	**6**
39.	Тема 7.1. Общие понятия об устройствеWiFi-сетей	0,5	0,5	1
40.	Тема 7.2. Угрозы безопасности WiFi-сетей	0,5	0,5	1
41.	Тема 7.3. Сниффинг	0,5	0,5	1
42.	Тема 7.4. Методы защиты сетей WiFi. Меры безопасности для пользователя WiFi.	0,5	0,5	1
43.	Тема 7.5. Настройка безопасностисетей WiFi	0,5	0,5	1
44.	Тема 7.6. Онлайн сервисы для безопасности пользователя в интернете.	0,5	0,5	1
	Кейс 8. Обработка и анализ большихданных. Основные принципы построения нейросетей.	**8**	**4**	**12**
45.	Тема 8.1. Определение больших данных, характеристики, сферыприменения.	2	0	2

46.	Тема 8.2. Процесс анализа. Общая схема анализа. Извлечение ивизуализация данных.	2	0	2
47.	Тема 8.3. Реальное применение и перспективы использованиятехнологии BIG DATA.	1	1	2
48.	Тема 8.4. Принципы машинного обучения. Основы построения нейросетей.	2	0	2
49.	Тема 8.5. Место нейрокомпьютеров в современных информационных технологиях.	1	1	2
50.	Тема 8.6. Представление результатовпроделанной работы.	0	2	2
	Итого	**34**	**38**	**72**

СОДЕРЖАНИЕ ПРОГРАММЫ «КИБЕРГИГИЕНА И РАБОТА С БОЛЬШИМИ ДАННЫМИ»

Кейс 1. Основы анализа информации в интернет-пространстве.

В рамках кейса 1 учащиеся научатся анализировать информацию в интернет-пространстве, исходя из информационной структуры интернета. Задача кейса основывается на структурировании и оценке информации в глобальной сети «Интернет». Проблемная ситуация подводит учащихся к необходимости изучения правил эффективного поиска и анализа информации в интернете. Учащимся будет предложено познакомиться с понятием информация, большие данные и принципами эффективного поискаинформации в интернете с помощью или без системы «Крибрум».

Учащиеся должны знать:

– и применять методы обработки информации;
– особенности и закономерности эффективного поиска информации винтернете.

Учащиеся должны уметь:

– планировать исследование;
– работать в системах совместного редактирования документов;
– строить таблицы и диаграммы для визуализации данных исследования;
– искать информацию в интернет-пространстве при помощи системы «Крибрум»;

– проводить контент-анализ;
– описывать и резюмировать результаты исследования;
– создавать презентации;
– работать в команде и давать обратную связь;
– представлять свой проект, свою команду и себя (навыки публичных выступлений);
– использовать интернет-пространство для формирования целостного представления о сложном феномене.

Формы занятий, используемые при изучении данного модуля:

- интерактивная лекция,
- практическая работа,
- самостоятельная работа,
- конференция.

Тема 1.1. Информационная структура интернета, поисковые системы.

Теория. Информационная структура интернета, поисковые системы.

Постановка задачи исследования.

Практика. Информационная структура интернета, поисковые системы. Знакомство с поисковыми системами на практике.

Тема 1.2. Принципы эффективного поиска информации в интернете. Принципы оценки качества источников информации.

Теория. Принципы эффективного поиска информации в интернете. Принципы оценки качества источников информации.

Практика. Использование эффективного поиска информации в интернете.Принципы оценки качества источников информации с помощью системы «Крибрум»

Тема 1.3. Определение больших данных. Технологии хранения большихданных

Теория. Определение больших данных. Технологии хранения большихданных.

Практика. Поиск больших данных. Технологии хранения больших данных.

Форма подведения итогов: публичное представление результатов исследований.

Кейс 2. Угрозы в интернет-пространстве, методы противодействия.

В рамках кейса 2 учащиеся научатся определять кибератаки и сбои в системе. Задача кейса основывается на анализе информации о способах защитыот вредоносного программного обеспечения. Проблемная ситуация подводит учащихся к необходимости рассматривать и принимать во внимание меры защиты программного обеспечения, изучению способов профилактики и лечения вирусов. Учащимся будет предложено оценить способы заражения компьютера при помощи системы «Крибрум» и без нее.

Учащиеся должны знать:

- и применять методы обработки информации.

Учащиеся должны уметь:

- планировать исследование;
- работать в системах совместного редактирования документов;
- строить таблицы и диаграммы для визуализации данных исследования;
- строить картограммы для визуализации данных исследования;
- выявлять и оценивать вредоносного программного обеспечения;
- выявлять опасности пользования онлайн-платежами;
- описывать и резюмировать результаты исследования;
- создавать презентации;
- работать в команде и давать обратную связь;
- представлять свой проект, свою команду и себя (навыки публичных выступлений);
- использовать интернет-пространство для формирования целостного представления о ситуации и выделения ключевых событий.

Формы занятий, используемые при изучении данного модуля:

- интерактивная лекция,
- практическая работа,
- самостоятельная работа,
- конференция.

Тема 2.1. Вирусные атаки ПК. Классы вирусов, способы защиты. Изучениесообщений о вирусных атаках с помощью системы «Крибрум».

Теория. Вирусные атаки ПК. Классы вирусов, способы защиты.

Практика. Изучение сообщений о вирусных атаках с помощью системы «Крибрум».

Тема 2.2. Антивирусные программы. Методология выбора оптимальнойантивирусной программы для личного ПК.

Теория. Антивирусные программы. Методология выбора оптимальнойантивирусной программы для личного ПК.

Практика. Методология выбора оптимальной антивирусной программыдля личного ПК. Установка и настройка антивируса

Тема 2.3. Фейковые сообщения и вредоносное ПО в сети Интернет.

Теория. Фейковые сообщения и вредоносное ПО в сети Интернет.

Практика. Поиск фейковых сообщений в сети Интернет.

Тема 2.4. Хакерские атаки, виды атак. Исследование юридических аспектов проблемы хакерства с помощью поисковых систем.

Теория. Хакерские атаки, виды атак. Исследование юридических аспектов проблемы хакерства с помощью поисковых систем.

Практика. Хакерские атаки, виды атак. Исследование юридических аспектов проблемы хакерства с помощью поисковых систем с помощью системы «Крибрум».

Тема 2.5. Проблема краж персональных данных с помощью вредоносного ПО. ПО.

Теория. Проблема краж персональных данных с помощью вредоносного

Практика. Изучение сообщений с помощью системы «Крибрум» проблема краж персональных данных с помощью вредоносного ПО.

Тема 2.6. Проблема краж с помощью банковских карт.

Теория. Проблема краж с помощью банковских карт.

Практика. Исследование сообщений в системе «Крибрум» проблема краж с помощью банковских карт.

Тема 2.7. Представление результатов проделанной работы.

Форма подведения итогов: публичное представление результатов исследований.

Кейс 3. Основы работы в социальных сетях.

В рамках кейса 3 учащиеся познакомятся с понятиями социальные сети и социальные медиа, научатся определять особенности социальных групп, исходя из их самопрезентации и поведения в социальных сетях. Задача кейса основывается на анализе соц. сети и фанатских сообществ. Проблемная ситуация подводит учащихся к необходимости изучения соц.сети, жизни сообщества и ситуаций, в которые оно вовлечено, для его оценки. Учащимися будет проанализирована актуальная информация о фанатских сообществах в различных источниках и их группы в социальных сетях при помощи системы «Крибрум» и без.

Учащиеся должны знать:

- и применять методы обработки информации;
- особенности и закономерности функционирования социальных групп на основе различных интернет-источников, поведенческих особенностей, предпочтений и интересов сообщества.

Учащиеся должны уметь:

- планировать исследование;
- работать в системах совместного редактирования документов;
- строить таблицы и диаграммы для визуализации данных исследования;
- искать информацию в интернет-пространстве при помощи системы «Крибрум»;

– проводить контент-анализ;
– описывать и резюмировать результаты исследования;
– создавать презентации;
– работать в команде и давать обратную связь;
– представлять свой проект, свою команду и себя (навыки публичных выступлений);
– использовать интернет-пространство для формирования целостного представления о сложном феномене.

Формы занятий, используемые при изучении данного модуля:

– интерактивная лекция,
– практическая работа,
– самостоятельная работа,
– конференция.

Тема 3.1. Социальные сети и социальные медиа.

Теория. Понятие социальные сети и социальные медиа.

Практика. Изучение сообщений о социальных сетях и социальныхмедиа с помощью системы «Крибрум».

Тема 3.2. Поведение молодежи в сети, проблема лайков.

Теория. Поведение молодежи в сети, проблема лайков.

Практика. Поведение молодежи в сети, проблема лайков. Изучениесообщений о поведении молодежи в социальных сетях с помощью системы «Крибрум».

Тема 3.3. Понятие социальная группа, сообщество, субкультура. Правила функционирования сетевых сообществ. Правила сетевого общения.

Теория. Понятие социальная группа, сообщество, субкультура. Правила функционирования сетевых сообществ. Правила сетевого общения.

Практика. Анализ с помощью системы «Крибрум» активности участников группы сообщества, связей, поведенческих особенностей, предпочтений и интересов сообщества (в том числе с использованием контент-анализа); подготовка к представлению результатов проделанной работы.

Тема 3.4. Представление результатов проделанной работы

Форма подведения итогов: публичное представление результатов исследований.

Кейс 4. Безопасное и рациональное использование личных и персональных данных в социальных сетях.

В рамках кейса 4 учащиеся научатся определять по аккаунтам в социальных сетях социально-демографические характеристики и индивидуальные особенности человека, распознавать признаки рискованного и опасного поведения, рационально и безопасно использовать в социальных сетяхличные и персональные данные. Задача кейса основывается на анализе собственного профиля в социальных сетях. Проблемная ситуация подводит учащихся к необходимости проверки личных и персональных данных, указанных в их аккаунтах, и при необходимости редактирования этих данных. Учащимся будет предложено изучить собственный аккаунт, в том числе при помощи системы «Крибрум», и сделать заключение о том, что стоит скорректировать. Также учащимся будут продемонстрированы примеры и последствия необдуманного размещения личных данных в социальных сетях. В заключение учащимся предлагается разработать рекомендации по безопасному и рациональному использованию личных и персональных данных в социальныхсетях.

Учащиеся должны знать:

– и применять методы обработки информации;
– принципы создания безопасных паролей и их хранения;

– принципы безопасного и рационального использования личных и персональных данных в социальных сетях.

Учащиеся должны уметь:

– планировать исследование;
– работать в системах совместного редактирования документов;
– строить таблицы и диаграммы для визуализации данных исследования;
– выявлять индивидуальные особенности пользователя в системе «Крибрум»;
– проводить контент-анализ;
– выявлять проблемы утечки данных, действия при взломе аккаунтов;
– исследовать аккаунты в социальных сетях с использованием контент-анализа, анализировать личные профили в социальных сетях;
– описывать и резюмировать результаты исследования;
– готовить презентацию и другие материалы для публичного представления;
– работать в команде и давать обратную связь;
– представлять свой проект, свою команду и себя;
– определять социально-демографические характеристики и индивидуальные особенности людей на основе аккаунтов в социальных сетях;
– создавать позитивный имидж в социальных сетях.

Формы занятий, используемые при изучении данного модуля:

– интерактивная лекция,
– практическая работа,
– самостоятельная работа,
– конференция.

Тема 4.1. Защищенность данных в сети. Проблемы утечки данных.

Теория. Защищенность данных в сети. Проблемы утечки данных. Действия при взломе аккаунтов. Безопасные пароли. Понятие персональных данных. Законодательство о защите персональных данных.

Практика. Подготовка к групповой работе по разработке рекомендаций по рациональному и безопасному использованию личных и персональных данных в социальных сетях. Разработка рекомендаций по созданию безопасных паролей и их хранению.

Тема 4.2. Создание безопасных паролей.

Теория. Принципы и методы создания безопасных паролей.

Практика. Работа с сервисами для создания паролей, менеджеры хранениянаролей.

Тема 4.3. Социальные сети: пользовательские соглашения, права и обязанности.

Теория. Политика социальных сетей в области конфиденциальности пользовательских данных.

Практика. Изучение пользовательских соглашений и политики безопасности социальных сетей.

Тема 4.4. Структура аккаунта пользователя социальной сети. Самопрезентация пользователя в социальных сетях. Проблема репостов, юридический аспект.

Теория. Структура аккаунта пользователя социальной сети.

Практика. Настройки приватности в социальных сетях. Самопрезентация пользователя в социальных сетях.

Тема 4.5. Проблемы использования в сообщениях геотегов.

Теория. Риски нерационального и небезопасного использования личных иперсональных данных в социальных сетях. Проблемы использования всообщениях геотегов, столкновения с неразумным и агрессивным поведением всети.

Практика. Анализ сообщений с использованием системы «Крибрум».

Тема 4.6. Исследование аккаунтов в социальных сетях с использованием контент-анализа, анализ личных профилей в социальных сетях.

Практика. Исследование аккаунтов в социальных сетях с использованием контент-анализа, анализ личных профилей в социальных сетях. Анализ сообщений с использованием системы «Крибрум».

Тема 4.7. Представление результатов проделанной работы

Форма подведения итогов: публичное представление результатовисследований.

Кейс 5. Распознавание опасного и вредного контента в интернет-пространстве.

В рамках кейса 5 учащиеся научатся распознавать опасный контент (фишинг, мошенничество, вовлечение в опасные виды деятельности), определять его источники и каналы распространения, а также узнают, как противодействовать угрозам интернет-пространства, и усвоят правила безопасного поведения в социальных сетях. Задача кейса основывается на анализе подозрительных объявлений в социальных сетях. Проблемная ситуация подводит учащихся к необходимости критически оценивать информацию, призывающую к каким-либо действиям. Учащимся будет предложено проанализировать распространение в социальных сетях объявлений о сборе средств, конкурсах, акциях, продаже товаров, дарении, услугах экстрасенсов при помощи системы «Крибрум», а также проверить достоверность данных объявлений. В заключение учащимся будет предложено алгоритмизировать действия при столкновении с подозрительным контентом в интернете и представить их на интеллект-карте.

Учащиеся должны знать:

- и применять методы обработки информации;
- как распознать опасный и вредный контент и людей с опаснымповедением по аккаунтам в социальных сетях.

Учащиеся должны уметь:

- планировать исследование;
- работать в системах совместного редактирования документов;
- строить таблицы и диаграммы для визуализации данных исследования;
- искать информацию в интернет-пространстве при помощи системы «Крибрум»;
- описывать и резюмировать результаты исследования;
- строить интеллект-карт;
- выявлять аккаунты (людей и групп), транслирующих опасный ивредный контент и демонстрирующих опасное поведение в социальных сетях;
- работать в команде и давать обратную связь;
- представлять свой проект, свою команду и себя (навыки публичных выступлений);
- использовать интернет-пространство для формирования целостного представления о сложном феномене.

Формы занятий, используемые при изучении данного модуля:

- интерактивная лекция,
- практическая работа,
- самостоятельная работа,
- конференция.

Тема 5.1. Проблема контентных рисков и меры противодействия им.

Теория. Проблема контентных рисков и меры противодействия им.

Механизмы защиты социальных сетей от негативного контента.

Практика. Постановка задачи исследования по подготовке интеллектуальной карты реагирования при столкновении с подозрительным контентом в сети.

Тема 5.2. Правила противодействия фишингу. Исследование фишинговых и коротких ссылок с помощью системы «Крибрум».

Теория. Проблема фишинга в сети. Правила противодействия фишингу.

Практика. Исследование фишинговых и коротких ссылок с помощью системы «Крибрум».

Тема 5.3. Интернет-коммерция. Площадки для Интернет-торговли. Проверка подлинности интернет-магазина.

Теория. Проблемы торговли через сеть Интернет. Популярные площадки. Мошеннические схемы, применяемы при работе на оналйн-площадках для торговли.

Практика. Методы опознания поддельных интернет-магазинов. Поиск мошеннических интернет-магазинов, объявлений о продаже.

Тема 5.4. Благотворительность с помощью интернет.

Теория. Благотворительность с помощью интернет. Методы опознания подлинного сайта благотворительного фонда.

Практика. Исследование с помощью «Крибрум» подозрительных объявлений о пожертвованиях в благотворительные фонды и частных сборах на лечение. Сравнение сайтов благотворительных фондов - опознание подлинности.

Тема 5.5. Риски потребительского поведения. Объявления о дарении, конкурсы репостов.

Теория. Рекомендации по проверке добросовестности организаторов конкурсов и акций.

Практика. Исследование объявлений о дарении и конкурсов репостов всоциальных сетях с помощью системы «Крибрум».

Тема 5.6. Проблема оказания поддельных услуг и распространения подозрительных объявлений об удаленной работе в социальных сетях.

Теория. Проблема оказания поддельных услуг и распространения подозрительных объявлений об удаленной работе в социальных сетях.

Практика. Анализ подозрительных сообщений с использованием системы «Крибрум», составление интеллектуальной карты действий при столкновении сподозрительным контентом.

Тема 5.7. Правила социальных сетей по размещению рекламы.

Теория. Основные правила размещения рекламы в социальных сетях. Отличие рекламы от публикаций в социальных сетях.

Практика. Работа SMM-специалиста. Изучение законодательства.

Тема 5.8. Сетевые игры: польза и вред.

Теория. История развития компьютерных игр, их виды и влияние на развитие и здоровье школьников. Для чего может быть полезен ПК и Интернети как польза превращается во вред.

Практика. Сетевые игры как массовые развлечения. Бесплатные и платные игры. Исследование популярных сетевых игр с помощью системы «Крибрум».

Тема 5.9. Киберугрозы Интернета. Кибертерроризм и кибервойны.

Теория. Понятие кибертерроризма и кибервойны. Деятельность кибервойск. Методы защиты от кибератак.

Практика. Анализ самых громких кибератак.

Тема 5.10. Кибершпионаж. Кибероружие.

Теория. Понятие и типы кибероружия. Кибершпионаж при помощи вредоносного программного обеспечения. Промышленный кибершпионаж.

Практика. Обнаружение и исследование вредоносных программ, относящихся к кибероружию.

Тема 5.11. Борьба с использованием Интернета в террористических, сепаратистских и экстремистских целях. Интернет как оружие массового поражения.

Теория. Понятие экстремизма, сепаратизма и терроризма. Почему сеть интернет идеально подходит для пропаганды.

Практика. Законодательные и организационные меры, направленные на борьбу с распространение террористических, сепарастических и экстремистских материалов в интернет.

Тема 5.12. Понятие интернет-зависимости, компьютерной зависимости и причин их возникновения.

Теория. Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости.

Практика. Методы предотвращения появления зависимости. Критическая оценка информации, получаемой из сети Интернет.

Тема 5.13. Развлечения в Интернет. Признаки зависимости. Сайты знакомств. Управление личностью через сеть. Киберкультура и личность. Типыинтернет-зависимости.

Теория. Деструктивная информация в Интернете – как ее избежать. Психологическое воздействие информации на человека. Столкновение с неразумным и агрессивным поведением в сети.

Практика. Критерии зависимости с точки зрения психологов. Как развивается зависимость. Интернет как наркотик. Классификация интернет- зависимостей. Опрос-выявление интернет-зависимости у учащихся).

Тема 5.14. Представление результатов проделанной работы

Форма подведения итогов: публичное представление результатовисследований.

Кейс 6. Безопасность мобильных устройств.

В рамках кейса 6 учащиеся научатся распознавать источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты). Рассмотрят угрозы для IOS-устройств и Android-устройств, изучат вирусы мобильных устройств (мобильные банкеры и др.) и методы борьбы с ними. Задача кейса основывается на анализе собственного мобильного устройства. Проблемная ситуация подводит учащихся к необходимости принятия мер для защиты своих данных. В заключение учащимся будет предложено алгоритмизировать действия по защите своего мобильного устройства и представить их на интеллект-карте.

Учащиеся должны знать:

- источники заражения мобильных устройств;
- как отражать и предотвращать атаки на устройства.

Учащиеся должны уметь:

- планировать исследование;
- работать в системах совместного редактирования документов;
- строить таблицы и диаграммы для визуализации данных исследования;
- описывать и резюмировать результаты исследования;
- строить интеллект-карт;
- выявлять аккаунты (людей и групп), транслирующих опасный ивредный контент и демонстрирующих опасное поведение в социальных сетях;
- работать в команде и давать обратную связь;
- представить свой проект, свою команду и себя (навыки публичныхвыступлений);
- использовать интернет-пространство для формирования целостного представления о сложном феномене.

Формы занятий, используемые при изучении данного модуля:

- интерактивная лекция,
- практическая работа,
- самостоятельная работа,
- конференция.

Тема 6.1. Безопасность мобильных устройств в информационных системах.

Теория. Операционные системы для мобильных устройств. Факторыриска для владельцев мобильных устройств.

Практика. Сравнительный анализ популярных ОС.

Тема 6.2. Источники заражения мобильных устройств.

Теория. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты).

Практика. Популярные типы вредоносного мобильного ПО.

Тема 6.3. Угрозы для IOS-устройств. Угрозы для Android-устройств.

Теория. Сравнительный анализ мобильных операционных систем IOS иAndroid.

Практика. Распространенные виды угроз для IOS-устройств и Android-устройств.

Тема 6.4. Рост числа угроз для мобильных устройств. Вирусы длямобильных устройств.

Теория. Типы вирусов мобильных устройств (мобильные банкеры и др.) иметоды борьбы с ними.

Практика. Проверка на безопасность различных приложений, установка,удаление. Работа с антивирусом на мобильном телефоне.

Тема 6.5. Представление результатов проделанной работы.

Форма подведения итогов: публичное представление результатов исследований.

Кейс 7. Угрозы безопасности в сетях WiFi. Онлайн сервисы безопасности.

В рамках кейса 7 учащиеся изучат общие понятия о работе с сетями WiFi, научатся распознавать угрозы безопасности WiFi-сетей, рационально и безопасно использовать сервисы для проверки безопасности пользователя (проверка компьютера и файлов на вирусы онлайн, онлайн деактивация SMS-вирусов, проверка сайта на вирусы, проверка файлов по e-mail, определение адреса страницы, проверка стоимости СМС и др.). Задача кейса основывается на анализе сети WiFi в ЦЦО IT-Куб. Проблемная ситуация подводит учащихся к необходимости использования сервисов для безопасности пользователя винтернете и настройке безопасности в сетях WiFi. Учащимся будет предложено изучить сеть WiFi в ЦЦО IT-Куб, сделать анализ и составить мнение о том, естьли угрозы данной сети.

Учащиеся должны знать:

- и применять методы защиты сетей WiFi;
- принципы настройки безопасности сетей WiFi, пользователя в интернете.

Учащиеся должны уметь:

- планировать исследование;
- работать в системах совместного редактирования документов;
- строить таблицы и диаграммы для визуализации данных исследования;
- проверять компьютер и файлы на вирусы онлайн, онлайн деактивация SMS-вирусов, проверка сайта на вирусы, проверка файлов по e-mail, определение адреса страницы, проверка стоимости СМС;
- описывать и резюмировать результаты исследования;
- готовить презентацию и другие материалы для публичного представления;

– работать в команде и давать обратную связь;
– представлять свой проект, свою команду и себя;
– определять социально-демографические характеристики и индивидуальные особенности людей на основе аккаунтов в социальных сетях;
– создавать позитивный имидж в социальных сетях.

Формы занятий, используемые при изучении данного модуля:

- интерактивная лекция,
- практическая работа,
- самостоятельная работа,
- конференция.

Тема 7.1. Общие понятия об устройстве WiFi-сетей.

Теория. Передача информации по беспроводному интерфейсу IEEE 802.11.

Практика. Точки доступа AP (Access Point).

Тема 7.2. Угрозы безопасности WiFi-сетей.

Теория. Прямые и косвенные угрозы. Опасности при работе с открытымиWiFi-сетями.

Практика. Разработка рекомендаций по безопасной работе в открытыхWiFi-сетях.

Тема 7.3. Сниффинг.

Теория. Сетевая атака, сниффинг пакетов. Понятие сниффинга, правовоерегулирование.

Практика. Работа сниффера на примере незащищенного соединения http.

Тема 7.4. Методы защиты сетей WiFi. Меры безопасности для пользователя WiFi. Настройка безопасности.

Теория. Типы шифрования в Wi-Fi. Методы ограничения доступа. Методы аутентификации.

Практика. Установка и настройка Wi-Fi-роутера.

Тема 7.5. Настройка безопасной WiFi-сети.

Теория. Атаки на сети WiFi.

Практика. Установка и настройка Wi-Fi-роутера.

Тема 7.6. Онлайн сервисы для безопасности пользователя в интернете.

Теория. Знакомство с полезными онлайн сервисами для безопасности пользователя в интернете.

Практика. Проверка компьютера и файлов на вирусы онлайн, онлайндеактивация SMS-вирусов, проверка сайта на вирусы, проверка файлов по e- mail, определение адреса страницы, проверка стоимости СМС.

Тема 7.7. Представление результатов проделанной работы.

Форма подведения итогов: публичное представление результатов исследований.

Кейс 8. Обработка и анализ больших данных. Основные принципы построениянейросетей.

В рамках кейса 8 учащиеся научатся определять большие данные и основные принципы построения нейросетей. Проблемная ситуация подводит учащихся к необходимости ознакомления с большими данными. Учащимся будет предложено изучить теоретический материал, в том числе при помощи системы «Крибрум», и иметь представление про большие

данные. Также учащимся будут продемонстрированы примеры больших данных и нейросетей.

Учащиеся должны знать:

– и применять методы обработки информации;
– принципы безопасного и рационального использования личных иперсональных данных в социальных сетях.

Учащиеся должны уметь:

– планировать исследование;
– работать в системах совместного редактирования документов;
– строить таблицы и диаграммы для визуализации данных исследования;
– выявлять индивидуальные особенности пользователя в системе «Крибрум»;
– проводить контент-анализ;
– выявлять большие данные;
– исследовать нейросети;
– описывать и резюмировать результаты исследования;
– создавать презентацию и другие материалы для публичного представления;
– работать в команде и давать обратную связь;
– представлять свой проект, свою команду и себя;
– определять социально-демографические характеристики и индивидуальные особенности людей на основе аккаунтов в социальных сетях;
– создавать позитивный имидж в социальных сетях.

Формы занятий, используемые при изучении данного модуля:

– интерактивная лекция,
– практическая работа,
– самостоятельная работа,
– конференция.

Тема 8.1. Определение больших данных, характеристики, сферы применения.

Теория. Определение больших данных, характеристики, сферы применения.

Тема 8.2. Процесс анализа. Общая схема анализа. Извлечение и визуализация данных.

Теория. Процесс анализа. Общая схема анализа. Извлечение и визуализация данных.

Тема 8.3. Реальное применение и перспективы использования технологииBIG DATA.

Теория. Реальное применение и перспективы использования технологииBIG DATA. Работа аналитика.

Практика. Работа с реальным применением технологии BIG DATA.

Тема 8.4. Принципы машинного обучения. Основы построения нейросетей.

Теория. Принципы машинного обучения. Основы построения нейросетей.

Тема 8.5. Место нейрокомпьютеров в современных информационныхтехнологиях.

Теория. Место нейрокомпьютеров в современных информационных технологиях.

Практика. Место нейрокомпьютеров в современных информационныхтехнологиях.

Форма подведения итогов: публичное представление результатов исследований.

Планируемые результаты освоения программы

Личностные:

- сформировать устойчивый интерес к правилам здоровье сберегающего и безопасного поведения;
- сформировать умение проявлять в самостоятельной деятельности валеологическую культуру и компетентность;
- сформировать умение вести себя сдержанно и спокойно.

Развивающие:

- развить творческую активность;
- развить умение представлять результаты своей работы окружающим, аргументировать свою позицию;
- развить аналитическое, практическое и логическое мышление;
- развить самостоятельность и самоорганизацию;
- развить умение работать в команде, развить коммуникативныенавыки;
- развить познавательную активность.

Социальные:

- сформировать умение пользоваться приемами коллективного творчества;
- сформировать умение эстетического восприятия мира и доброе отношение к окружающим.

Регулятивные:

- сформировать умение соотносить свои действия с планируемыми результатами, осуществлять контроль своей деятельности в процессе достижения результата;
- сформировать умение определять способы действий в рамках предложенных условий и требований, корректировать свои действия в соответствии с изменяющейся ситуацией.

Познавательные:

- сформировать умение работать с литературой и другими источниками информации;
- сформировать умение самостоятельно определять цели своего обучения.

Коммуникативные:

- сформировать умение организовать учебное сотрудничество и совместную деятельность с педагогом и сверстниками;
- сформировать умение работать индивидуально и в группе, уметь вступать в контакт со сверстниками.

Предметные:

- владеть основными приемами работы в прикладных программах для обработки информации;
- сформировать представление о структуре и типах информации в интернет-пространстве, больших данных и больших пользовательских данных;
- познакомить с методами и средствами поиска информации в интернет-пространстве;

- сформировать навыки планирования, проведения и обработки результатов исследования информации в интернет-пространстве при помощи поисковых систем, общедоступных средств поиска информации и системы мониторинга и анализа социальных медиа «Крибрум»;
- сформировать у учащихся способность выявлять и критически оценивать источники и каналы распространения информации в интернет-пространстве и определять ее качество;
- сформировать способность определять социальные характеристики и индивидуальные особенности людей и обнаруживать признаки опасного поведения на основании их аккаунтов в социальных сетях;
- сформировать способность к успешной самопрезентации и формированию позитивного имиджа в социальных сетях;
- сформировать у учащихся способность распознавать опасный и вредный контент и идентифицировать явления манипулирования сознанием в интернет-пространстве, внушения деструктивных идей и вовлечения в социально опасные группы в социальных сетях;
- обучить приемам противодействия негативным воздействиям в интернет-пространстве;
- сформировать культуру позитивного использования интернет-пространства.

Метапредметные:

- ориентироваться в своей системе знаний: отличать новое знание от известного;
- перерабатывать полученную информацию: делать выводы в результате совместной работы группы, сравнивать и группировать предметы и их образы;
- работать по предложенным инструкциям и самостоятельно;
- излагать мысли в четкой логической последовательности, отстаивать свою точку зрения, анализировать ситуацию и самостоятельно находить ответы на вопросы путем логических рассуждений;
- определять и формировать цель деятельности на занятии с помощью учителя;
- уметь рассказывать о проекте;
- работать над проектом в команде, эффективно распределять обязанности;
- работать над проектом индивидуально, эффективно распределять время.

Способы определения результативности

Педагогическое наблюдение, педагогический анализ результатов решения задач, результаты участия в интеллектуальных конкурсах всероссийского уровня.

Результатом работы над каждым кейсом должна стать презентация (общая для всей группы или своя в каждой малой группе) или общий документ в другом формате (интеллект-карта, лента времени, видеоролик и т.д.).

Виды контроля:

- устный опрос;
- самостоятельная работа;
- участие в проектной деятельности.

Формы подведения итогов реализации программы

По окончании обучения проводится итоговая аттестация в форме публичной защиты проектов.

Нормативная база.

- Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 31.07.2020) «Об образовании в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2020).
- Приказ Министерства просвещения Российской Федерации от 31.05.2021 № 287 «Об утверждении федерального государственного образовательного стандарта основного общего образования» (Зарегистрирован 05.07.2021 № 64101).
- Приказ Министерства просвещения Российской Федерации № 568 от 18.07.2022 "О внесении изменений в федеральный государственный образовательный стандарт основного общего образования" (Зарегистрирован 17.08.2022 № 69675).
- Приказ Министерства просвещения Российской Федерации от 12.08.2022 № 732 "О внесении изменений в федеральный государственный образовательный стандарт среднего общего образования, утвержденный приказом Министерства образования и науки Российской Федерации от 17 мая 2012 г. № 413" (Зарегистрирован 12.09.2022 № 70034).
- Приказ Министерства просвещения Российской Федерации от 02.08.2022 № 653 "Об утверждении федерального перечня электронных образовательных ресурсов, допущенных к использованию при реализации имеющих государственную аккредитацию образовательных программ начального общего, основного общего, среднего общего образования" (Зарегистрирован 29.08.2022 № 69822).
- Паспорт национального проекта «Образование» (утверждён президиумом Совета при Президенте РФ по стратегическому развитию и _национальным проектам, протокол от 24.12.2018 № 16).
- Государственная программа Российской Федерации «Развитие образования» (утверждена постановлением Правительства РФ от 26.12.2017 № 1642 (ред. от 22.02.2021) «Об утверждении государственной программы Российской Федерации «Развитие образования»).
- Стратегия развития воспитания в Российской Федерации на период до 2025 года (утверждена распоряжением Правительства РФ от 29.05.2015 № 996-р «Об утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 года»).
- Постановление Главного государственного санитарного врача Российской Федерации от 28.09.2020 № 28 «Об утверждении санитарных правил СП 2.4. 3648-20 «Санитарно - эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи».
- Методические рекомендации по созданию и функционированию центров цифрового образования «IT-куб» (утверждены распоряжением Министерства

просвещения Российской Федерации от 12 января 2021 г. № Р-5).

- Методические рекомендации по созданию и функционированию в общеобразовательных организациях, расположенных в сельской местности и малых городах, центров образования естественно-научной и технологической направленностей («Точка роста») (утверждены распоряжением Министерства просвещения Российской Федерации от 12 января 2021 г. № Р-6).
- Распоряжение Правительства Ростовской области от 03.07.2019 № 376 «О создании и функционировании центров цифрового образования детей «IT-куб» в Ростовской области».

СПИСОК ИСТОЧНИКОВ ИНФОРМАЦИИ, использованных при написании программы:

1. Говор С.А., Теделури М.М., Шулаева О.В. Рабочая программа по направлению «Кибергигиена». – Москва, 2019 г.
Методическое пособие по направлению «Dataквантум». – Москва,2018