Министерство образования и науки Самарской области

Государственное бюджетное образовательное учреждение
дополнительного образования Самарской области
«Самарский областной центр детско-юношеского технического творчества»

Принята на заседании
Методического Совета
Протокол № 2

от «20» июня 2023 г.

УТВЕРЖДАЮ
Директор ГБОУ ДО СО СОЦДЮТТ

_____/А.Ю. Богатов/

«20» июня 2023 г.

Дополнительная общеобразовательная общеразвивающая программа технической направленности

«Кибергигиена и большие данные. Начальный уровень»

Возраст детей: 12-18 лет
Срок обучения: 1 год

Разработчик:
Милокумов Игорь Владиславович
педагог дополнительно образования
первой квалификационной категории

Самара, 2023

Оглавление

Пояснительная записка	3
Учебно-тематический план	6
Содержание	7
Методическое обеспечение	8
Список литературы	10
Приложение Календарно-тематическое планирование	11

Пояснительная записка

Дополнительная общеобразовательная программа «Кибергигиена и большие данные. Начальный уровень» является общеразвивающей программой ***технической*** направленности. Автор программы - Милокумов Игорь Владиславович.

Категория обучающихся: от 12 до 18 лет.

Количество часов реализации программы: 72 академических часа 2 часа в неделю.

Дополнительная общеобразовательная общеразвивающая программа технической направленности «Кибергигиена и большие данные. Начальный уровень» предназначена для формирования научного мировоззрения, развития прикладных, исследовательских способностей обучающихся, с наклонностями в области технического творчества.

Кибергигиена - это защищённость в информационном пространстве. На занятиях обучающиеся поймут структуру интернет-пространства, научатся разбираться в источниках и типах информации в интернете, освоят поисковые системы и средства поиска информации.

Актуальность. Интернет стал неотъемлемой частью жизни. В информационном пространстве возможно абсолютно все: приобретать товар, находить знакомых, необходимую информацию и т.д. Но часто пользователи сталкиваются с мошенничеством. Поэтому важно знать правила безопасности в интернете. Именно этому обучают на занятиях по дополнительной общеобразовательной программе технической направленности «Кибергигиена и большие данные. Начальный уровень».

Педагогическая целесообразность данной программы заключается в пробуждении интереса обучающихся к новому виду деятельности. Занятия по программе создают условия по освоению теоретических основ кибербезопасности. В процессе реализации программы, обучающиеся освоят основы кибергигиены.

Отличительная особенность программы состоит в том, что она в доступной форме знакомит учащихся со основами безопасности в информационной среде. В каждом кейсе программы присутствует как теоретическая, так и практическая часть, поэтому учащиеся будут видеть конкретный результат освоения предмета.

Адресат программы - дети от 12 до 18 лет. Наполняемость групп: 10 – 12 человек.

Объем и срок освоения программы. Дополнительная общеобразовательная технической направленности общеразвивающая программа «Кибергигиена и большие данные. Начальный уровень» рассчитана на 1 год обучения.

Режим занятий: 72 академических часа в год, 2 академических часа в неделю.

Форма реализации - очная. Имеется возможность проводить занятия в дистанционном формате через платформы для видеосвязи.

В каникулярное время занятия проводятся в соответствии с календарным учебным графиком, допускается изменение форм занятий, проведение воспитательных мероприятий.

Цель программы - формирование у обучающихся способности к разностороннему и комплексному анализу информации, размещенной на различных интернет-ресурсах, в интересах безопасного и рационального использования интернет-пространства.

Цель и задачи программы

Задачи программы:

Образовательные:

1. Сформировать у обучающихся представление о структуре и типах информации в интернет-пространстве больших данных и больших пользовательских данных;
2. Сформировать у учащихся способность выявлять и критически оценивать источники и каналы распространения информации в интернет-пространстве и определять ее качество;
3. 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;
4. Сформировать у учащихся навыки планирования, проведения и обработки результатов исследования информации в интернет-пространстве при помощи поисковых систем и общедоступных средств поиска информации.

Развивающие:

1. Развивать навыки поиска информации в интернет-пространстве;
2. Развивать способность к успешной само-презентации и формированию позитивного имиджа в социальных сетях;
3. Развить навыки исследовательской деятельности (принципами построения исследования, процедурой и этикой его проведения, количественными и качественными методами обработки полученных данных).

Воспитательные:

1. Воспитать умение работать в коллективе с учетом личностных качеств учащихся, психологических и возрастных особенностей;
2. Воспитать трудолюбие и уважительное отношения к интеллектуальному труду;

3. Сформировать у учащихся ответственное отношение к сохранению личной информации;

4. Сформировать мотивацию к профессиональному самоопределению учащихся.

Планируемые результаты и способы определения их результативности

1. Знание структуры интернет-пространства, знание типов источников информации и разновидностей контента;

2. понимание и применение правил безопасного поведения в интернет-пространстве, рационального использования персональных данных, защиты от вредоносных воздействий;

3. Умение работать с поисковыми системами, общедоступными средствами поиска информации в интернет-пространстве;

4. Умение анализировать информацию в интернет-пространстве при помощи количественных и качественных методов, формировать целостное представление об объекте, ситуации или социальной группе на основе разных источников.

Учебно-тематический план

Наименование кейса, темы	**Количество часов**		
	Теория	**Практика**	**Всего**
Основы кибергигиены. Анализ личной информации доступной в интернет-пространстве	4	4	8
Кейс 1. Распознавание опасного контента в интернет-пространстве	6	6	12
Кейс 2. Безопасное использование персональных данных в социальных сетях	6	6	12
Кейс 3. Анализ социальных групп на основе данных интернет-пространства	6	6	12
Кейс 4. Анализ мнений интернет-пользователей	8	8	16
Кейс 5. Ликвидация последствий сбоев системы и кибератак	6	6	12
Итого:	**36**	**36**	**72**

Содержание

Основы кибергигиены. Анализ личной информации доступной интернет-пространстве

Теория: Информационная структура интернета. Основы поиска в интернете. Раскрытие каналов утечки информации. Механизмы сайтов сбора информации о пользователе. Виды трекеров. В каких целях может быть использована собираемая сайтами информация. Цифровой отпечаток браузера.

Практика: учащиеся устанавливают и настраивают полезные расширения, предотвращающие утечку информации и проверяют их работу.

Кейс 1. Распознавание опасного контента в интернет-пространстве

Теория: Раскрытие понятия «фишинг». Виды «фишинга». Фишинговые сайты. Подозрительные письма. Мошенники в интернет пространстве. В каких целях может быть использована украденная информация. Изучение фейковых сообщений и вредоносного программного обеспечения (далее ПО) в сети интернет. Критическое мышление.

Практика: учащиеся распознают заранее подготовленный подозрительный контент, приводят личные примеры информационных атак из жизни.

Кейс 2. Безопасное использование персональных данных в социальных сетях

Теория: Раскрытие каналов утечки информации в социальных сетях. Структура аккаунта пользователя социальной сети. Настройки безопасности и конфиденциальности. Надёжный пароль и двухфакторная аутентификация. Способы получения скрытой информации и уязвимости социальных сетей.

Практика: учащиеся настраивают и обеспечивают безопасность своего аккаунта в социальной сети.

Кейс 3. Анализ социальных групп на основе данных интернет-пространства

Теория: Раскрытие понятия социальная группа. Виды социальных групп. Для чего может понадобится анализ социальных групп в интернет пространстве. Раскрытие понятия «большие данные». Основы работы с большими данными. Общедоступные бесплатные сервисы анализа сообществ в социальных сетях.

Практика: учащиеся анализируют сообщества в социальных сетях в поисках целевой аудитории. Даётся несколько заданий в которых целевая аудитория определяется разными критериями сначала наставником потом учащимися.

Кейс 4. Анализ мнений интернет-пользователей

Теория: Для решения каких задач может понадобится анализ мнений интернет пользователей. Раскрытие методов сбора хранения и обработки больших данных. Закон о персональных данных. Алгоритм составления и проведения опроса. Обработка результатов

в программе Microsoft Excel. Способы дистанционной командной работы. Сервисы для дистанционной командной работы.

Практика: Командное составление формы для анонимного интернет-опроса. Сбор результатов, обработка и анализ в программе Microsoft Excel.

Кейс 5. Ликвидация последствий сбоев системы и кибератак.

Теория: Раскрытие понятия «сбой системы». В результате каких действий может произойти сбой системы. Предотвращение сбоев системы и кибератак. Важность резервного копирования. Методы восстановления системы после сбоя. Создание загрузочного образа на USB-флеш-накопитель и средства восстановления.

Практика: учащиеся под руководством наставника устраняют сбой системы на заранее подготовленном компьютере. Учащиеся согласно инструкциям наставника настраивают систему для предотвращения дальнейших сбоев и кибератак.

Методическое обеспечение

Материально-техническое обеспечение

- персональный ноутбук
- мультимедийный проектор
- магнитно-маркерная доска
- программное обеспечение Microsoft Excel
- доступ в интернет

Методы и приемы работы

-сенсорное восприятие (лекции, просмотр видеофрагментов);

-практические (выполнение практических заданий);

-коммуникативные (дискуссии, беседы, ролевые игры);

-комбинированные (самостоятельная работа учащихся);

Контрольно-измерительный блок

Форма	Описание	Критерии оценки
Устный опрос	Групповая и индивидуальная беседа по пройденному материалу	Обучающийся должен иметь представление о основных пройденных темах и определениях
Практическое задание	Выполнение индивидуального или группового практического задания описанного в кейсе.	Обучающиеся должны уметь выполнять описанное в кейсе задание самостоятельно или в группе.

Список литературы

1. Богачева Т.Ю., Соболева А.Н., Соколова А.А. Риски интернет пространства для здоровья подростков и пути их минимизации // Наука для образования: Коллективная монография. М.: АНО «ЦНПРО», 2015.
2. Кравченко А.И. Методология и методы социологических исследований. Учебник. М.: Юрайт, 2016.
3. Солдатова Г.У., Шляпников В.Н., Журина М.А. Эволюция онлайн рисков: итоги пятилетней работы линии помощи «Дети онлайн» // Консультативная психология и психотерапия. 2015. № 3. С. 50-66.
4. Герцог Г.А. Основы научного исследования: методология, методика, практика: учебное пособие. Челябинск: Изд-во Челяб. гос. пед. ун та, 2018.
5. Ефимова Л.Л., Кочерга С.А. Информационная безопасность детей: российский и зарубежный опыт: Монография. М.: ЮНИТИ-ДАНА, 2016.
6. Слугина Н. Активные пользователи социальных сетей Интернета. СПб.: Питер, 2015.
7. Солдатова Г., Зотова Е., Лебешева М., Вляпников В. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. Ч. 1. Лекции. М.: Google, 2016.
8. Солдатова Г., Рассказова М., Лебешева М., Зотова Е., Рогендорф П. Дети России онлайн. Результаты международного проекта EU Kids Online II в России. М.: Фонд Развития Интернет, 2017.
9. Солдатова Г.У., Рассказова Е.И., Зотова Е.Ю. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования. М.: Фонд Развития Интернет, 2019.
10. Ашманов И.С. Идеальный поиск в Интернете глазами пользователя. М.: Питер, 2016.
11. Ашманов И.С., Иванов А.А. Продвижение сайта в поисковых системах. М.: Вильямс, 2017.
12. Баскаков А.Я., Туленков Н.В. Методология научного исследования: Учеб. пособие. К.: МАУП, 2015.

Приложение1

Календарно-тематическое планирование

Дата		№ занятия	Тема занятия	Кол-во часов
По плану	По факту			
		1	Основы кибергигиены. Информационная структура интернета.	2
		2	Основы кибергигиены. Основы поиска в интернете.	2
		3	Основы кибергигиены. Раскрытие каналов утечки информации. Механизмы сайтов сбора информации о пользователе. Виды трекеров.	2
		4	Основы кибергигиены. В каких целях может быть использована собираемая сайтами информация. Цифровой отпечаток браузера.	2
		5	Кейс 1. Раскрытие понятия «фишинг». Виды «фишинга».	2
		6	Кейс 1. Фишинговые сайты.	2
		7	Кейс 1. Подозрительные письма. Мошенники в интернет пространстве.	2
		8	Кейс 1. В каких целях может быть использована украденная информация.	2
		9	Кейс 1. Изучение фейковых сообщений и вредоносного ПО в сети интернет.	2
		10	Кейс 1. Критическое мышление.	2
		11	Кейс 2. Раскрытие каналов утечки информации в соц. сетях.	2
		12	Кейс 2. Структура аккаунта пользователя социальной сети.	2
		13	Кейс 2. Настройки безопасности и конфиденциальности.	2
		14	Кейс 2. Надёжный пароль и двухфакторная аутентификация.	2
		15	Кейс 2. Способы получения скрытой информации в социальных сетях	2
		16	Кейс 2. Уязвимости социальных сетей.	2
		17	Кейс 3. Раскрытие понятия социальная группа. Виды социальных групп.	2
		18	Кейс 3. Для чего может понадобится анализ социальных групп в интернет	2

			пространстве.	
		19	Кейс 3. Раскрытие понятия «большие данные».	2
		20	Кейс 3. Основы работы с большими данными.	2
		21	Кейс 3. Основы работы с большими данными.	2
		22	Кейс 3. Общедоступные бесплатные сервисы анализа сообществ в социальных сетях.	2
		23	Кейс 4. Для решения каких задач может понадобится анализ мнений интернет-пользователей.	2
		24	Кейс 4. Методы сбора и хранения больших данных.	2
		25	Кейс 4. Закон о персональных данных.	2
		26	Кейс 4. Алгоритм составления опроса.	2
		27	Кейс 4. Проведение опроса.	2
		28	Кейс 4. Обработка результатов в программе Microsoft Excel.	2
		29	Кейс 4. Способы дистанционной командной работы.	2
		30	Кейс 4. Сервисы для дистанционной командной работы.	2
		31	Кейс 4. Методы обработки больших данных.	2
		32	Кейс 5. Предотвращение сбоев системы и кибератак.	2
		33	Кейс 5. Важность резервного копирования.	2
		34	Кейс 5. Методы восстановления системы после сбоя.	2
		35	Кейс 5. Создание загрузочного образа на USB-флеш-накопитель.	2
		36	Аттетация	2
Итого				72