УТВЕРЖДАЮ
Директор по персоналу ООО «Рубиус»
(по Доверенности №02 от 01.01.2023)
_____ / Ольга Сергеевна Мальцева
«10» апреля 2023 г.

Учебно-тематическое планирование
к программе обучения «Кибербезопасность»

Количество часов
Всего – 48 академ. часа (32 аудиторных часов и 16 часов самостоятельной работы);
в неделю – 1 занятие
Длительность занятий – 60 минут
Итоговый контроль – 2 часа.

Пояснительная записка

Направленность программы: данная программа направлена на обучение детей основам кибербезопасности, которая охватывает понимание основных угроз в сфере информационных технологий и способы защиты от них. Курс предоставит детям знания и навыки, необходимые для безопасного поведения в цифровом мире.

Актуальность программы: с развитием технологий и увеличением числа пользователей интернета, кибербезопасность становится важным аспектом жизни каждого человека. Дети становятся активными участниками цифрового пространства и подвергаются различным киберугрозам. Понимание основ кибербезопасности поможет детям избежать опасных ситуаций и защитить свои личные данные.

Педагогическая целесообразность программы: обусловлена важностью кибербезопасности и необходимостью обучать детей основам защиты в цифровом мире. Программа способствует развитию критического мышления, ответственного поведения в онлайн-среде и умению реагировать на киберугрозы.

Цель данной программы: обучить детей основам кибербезопасности и подготовить их к безопасному поведению в интернете и сетях.

Задачи:

1. Образовательные:

- Познакомить учащихся с основными понятиями кибербезопасности и типами киберугроз.
- Обучить основным принципам безопасного использования интернета и социальных сетей.
- Ознакомить с методами защиты личной информации и паролей.

- Изучить основы обнаружения и предотвращения вредоносных программ.

2. Развивающие:

- Развивать критическое мышление и умение анализировать информацию из сети.
- Поддерживать интерес учащихся к темам кибербезопасности и информационной безопасности.
- Способствовать развитию коммуникационных навыков для общения об опасных ситуациях в сети.

3. Воспитывающие:

- Воспитывать ответственность за свои действия в интернете и защиту личных данных.
- Поддерживать сознательное отношение к использованию информационных технологий.
- Содействовать формированию этических принципов в цифровой среде.

Возраст обучающихся: 9-17 лет. Программа рассчитана на 6 месяцев обучения.

Результаты: по окончании курса учащиеся смогут:

- Понимать основные угрозы в сфере кибербезопасности и знать, как их предотвращать.
- Применять основные методы защиты личной информации в интернете.
- Безопасно использовать социальные сети и осознанно взаимодействовать с незнакомцами в сети.
- Определять и предотвращать вредоносные программы и мошеннические действия в сети.

Формы подведения итогов: способом определения результативности является успешное выполнение практических заданий, участие в обсуждениях по кибербезопасности и создание собственных рекомендаций по обеспечению безопасности в сети. Итоговый контроль осуществляется посредством проверки усвоенной информации и успешной демонстрации навыков защиты.

Формы деятельности:

- беседа с объяснением материала;
- Практические упражнения и задания.
  Проектные работы, включающие разработку сценариев безопасного поведения в сети.

В учебном процессе используются следующие **средства обучения:**

- Учебный кабинет с доступом к компьютерам и интернету для практических занятий.
- Учебные материалы, включая специализированные учебники и онлайн-ресурсы по кибербезопасности.

Текущий и итоговый контроль (аттестация)

В течение учебного периода – педагогическое наблюдение, опрос, проверочные задания и упражнения на изученную тему.
По окончании изучения темы или раздела – опрос, контрольное занятие.
В конце курса обучения – опрос, контрольное занятие.

Учебно-тематическое планирование

Разделы программы и темы занятий	Всего часов
Модуль 1. Введение в ИБ. 1. Целостность 2. Конфиденциальность 3. Доступность	6 часов
Модуль 2. Криптография. 1. Что такое криптография 2. Виды шифрования	8 часов
Модуль 3. Безопасность операционных систем. 1. Вирусы и трояны 2. Сетевые черви 3. Аутентификация и обход ограничений 4. Технические методы взлома паролей 5. Распределение прав 6. Фаерволы 7. VPN и прокси	8 часов
Модуль 4. Социальный инжениринг. 1. Понятие социального инжениринга 2. Психология и сценарии поведения 3. Списки контактов и социальные сети	8 часов
Модуль 5. Проводные и беспроводные сети. 1. OSI 2. Фишинг 3. Возможности внедрения	8 часов

4. Аутентификация на уровне устройств 5. Анализ локальной сети при подготовке к атаке или защите 6. Сетевые атаки. DoS, DDoS	
Модуль 6. Инструментарий специалиста. 1. Программы для смартфонов 2. Программы для Linux 3. Программы для Windows 4. Аппаратные средства. USB Rubber Ducky, WiFi Pinapple 5. Специализированные операционные системы. Kali Linux	8 часов
Итоговое занятие Защита командного проекта. Подведение итогов.	2 часа
Итого	**48 часов**

Содержание обучения

№ п/п	Тема	Количество часов		
		Всего	Теория	Практика
1	Введение в ИБ	6	2	4
2	Криптография	8	4	4
3	Безопасность операционных систем	8	4	4
4	Социальный инжениринг	8	4	4

5	Проводные и беспроводные сети	8	4	4
6	Инструментарий специалиста	8	4	4
7	Итоговое занятие	2	-	2
	ВСЕГО	**63 часа**	**21**	**42**

Учебная литература:

1. Взломать всё. Как сильные мира сего используют уязвимости систем в своих интересах. Брюс Шнайер, 2023 г.
2. Этичный хакинг. Практическое руководство по взлому. Дэниел Г. Грэм, 2021 г.
3. Ловушка для багов. Полевое руководство по веб-хакингу. Питер Яворски, 2019 г.
4. Поговорят и забудут. Как не дать интернет-агрессии разрушить репутацию, карьеру и жизнь. Надежда Кобина, Елена Старостина. 2023 г.
5. Как противостоять хакерским атакам. Уроки экспертов по информационной безопасности. Роджер Граймс, 2017 г.
6. Как оценить риски в кибербезопасности. Лучшие инструменты и практики, Дуглас У. Хаббард, Ричард Сирсен, 2016 г.
7. Информационная безопасность для пользователя. Правила самозащиты в Интернете. Михаил Райтман, 2023 г.