

Муниципальное автономное общеобразовательное учреждение «Лицей №9»
Асбестовского городского округа

Утверждено
приказом от 30.08.2020 № 204-од

Дополнительная общеобразовательная общеразвивающая программа
технической направленности
«Методы и технологии защиты информации»

срок обучения: 1 год
возраст обучающихся: 15-17 лет

Автор-составитель:
Роман Кириллович Михайдаров
учитель математики,

г.Асбест, 2020 год

1. Объем образовательной программы

Количество часов в месяц	Количество часов в год
4	18

2. Содержание программы

Понятие «защита информации».

Актуальность информационной безопасности. Основные аспекты. Историческая справка. Развитие угроз безопасности и статистика

Угрозы безопасности

«Некомпьютерные» угрозы безопасности данных. Вирусы и их характеристика. Методы работы. Отказ в обслуживании. Способы проникновения через уязвимости в ПО.

Меры защиты информации. Процедурный и административный методы.

Игра «Руководитель компании». Способы защиты информации. Пропускной режим. Ограниченный доступ к информации. Аутентификация данных. Политика безопасности. Законодательный уровень.

Криптографические методы защиты информации.

Предмет и задачи криптографии, требования к криптографическим системам защиты информации, пример простейшего шифра. Общая схема симметричного шифрования. Принципы построения блочных шифров с закрытым ключом. Алгоритмы шифрования DES и AES. Алгоритм криптографического преобразования данных ГОСТ 28147-89. Поточные шифры и генераторы псевдослучайных чисел. Криптографические алгоритмы с открытым ключом и их использование. Электронная цифровая подпись

3. Планируемые результаты

В результате освоения программы обучающийся научится:

- характеризовать современные направления в сфере информационных технологий; описывать их возможное использование в практической деятельности;
- избегать атак в области информационной безопасности;
- различать протоколы и спецификации в области информационной безопасности;
- шифровать информацию с использованием различных алгоритмов;
- создавать программы в одном из языков программирования;
- понимать различия в алгоритмах шифрования данных;
- выделять различные уровни информационной безопасности;
- создавать собственную программу для шифрования и дешифровки данных

4. Учебный план

№	Название раздела, темы	Количество часов			Формы аттестации, контроля
		Всего	Теория	Практика	
1	Актуальность защиты информации	1	1	0	Наблюдение
2	Угрозы безопасности. Стандарты и спецификации в области информационной безопасности	2	2	0	Наблюдение
3	Меры защиты информации. Административный и процедурные методы.	1	1	0	Наблюдение
4	Криптографические методы защиты информации.	11	7	4	Практическая работа
5	Итоговая практическая работа	3	0	3	Практическая работа
Итого		18	11	7	

5.Календарный учебный график

№	Форма занятия	Количество часов	Тема занятия	Место проведения занятия	Формы контроля
1	Групповая очная	1	Актуальность и потребность в информационной безопасности	Кабинет № 214	Фронтальный опрос
2	Групповая очная	1	Распространённые угрозы безопасности и меры по борьбе с ними	Кабинет № 214	Фронтальный опрос
3	Групповая очная	1	Стандарты и спецификации в области информационной безопасности	Кабинет № 214	Практическая работа
4	Групповая очная	1	Меры защиты информации. Административный и процедурные методы.	Кабинет № 214	Практическая работа
5	Групповая очная	1	Основные понятия криптографии	Кабинет № 214	Фронтальный опрос
6	Групповая очная	1	Простейшие методы шифрования с закрытым ключом	Кабинет № 214	Практическая работа
7	Групповая очная	1	Принцип построения блочных шифров с закрытым ключом	Кабинет № 214	Фронтальный опрос
8	Групповая очная	1	Практическая работа № 1 «Создание массива в выбранном языке программирования»	Кабинет № 214	Практическая работа
9	Групповая очная	1	Алгоритм шифрования DES, AES и ГОСТ 28147-89	Кабинет № 214	Фронтальный опрос
10	Групповая очная	1	Практическая работа №2 «Перестановки в массиве»	Кабинет № 214	Практическая работа
11	Групповая очная	1	Поточные шифры и генераторы псевдослучайных чисел	Кабинет № 214	Фронтальный опрос
12	Групповая очная	1	Практическая работа №3 «Создание закодированного сообщения»	Кабинет № 214	Фронтальный опрос
13	Групповая очная	1	Криптография с открытым ключом	Кабинет № 214	Лабораторная работа
14	Групповая очная	1	Практическая работа №4 «Создание механизма кодирования сообщения»	Кабинет № 214	Фронтальный опрос
15	Групповая очная	1	Электронная цифровая подпись. Сжатие информации.	Кабинет № 214	Фронтальный опрос
16	Групповая очная	3	Итоговая практическая работа	Кабинет № 214	Контрольная работа.

