МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «КАМЕНОЛОМНЕНСКАЯ СРЕДНЯЯ ШКОЛА» САКСКОГО РАЙОНА РЕСПУБЛИКИ КРЫМ

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
на заседании методического объединения учителей естественно-математического цикла Протокол №4 от «30» августа 2023 г.	заместителем директора МБОУ«Каменоломненская средняя школа» Протокол №14 от «30» августа 2023 г.	приказом МБОУ«Каменоломненская средняя школа» № 213 от «31» августа 2023 г.

РАБОЧАЯ ПРОГРАММА

По учебному курсу «Информационная безопасность» для обучающихся 11 класса

соответствует федеральной рабочей программе учебному курсу «Информационная безопасность» для среднего общего образования

Составитель: Шерматова Г.Ш.
Учитель информатики

2023 г.

Рабочая программа учебного курса «Информационная безопасность» (далее программа) предназначена для реализации в 11-х классах.

Программа углубляет знания, обучающихся по правовым основам информационной безопасности и направлена на совершенствование компетенций информационной безопасности личности.

Форма реализации программы – факультативные занятия. Общий объем учебного времени составляет 34 часов (по 1 часу в неделю) и рассчитан на один год обучения.

Программа разработана на основе учебных пособий «Кибербезопасность» и «Информационная безопасность. Правовые основы информационной безопасности» (Цветкова М.С., Якушина Е.В. – М.: БИНОМ. Лаборатория знаний, 2019»). Электронные приложения к пособиям представлены на сайте издательства «БИНОМ. Лаборатория знаний»: **http://lbz.ru/metodist/authors/ib/.**

Основной целью курса является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи курса:

- изучить правовые основы информационной безопасности;
- сформировать понимание сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности;
- рассмотреть основные методы обеспечения информационной безопасности;
- познакомить с особенностями реализации общих методик защиты информации на различных платформах;
- сформировать навыки защиты личного информационного пространства;
- развивать творческие способности обучающихся;
- готовить к участию в мероприятиях по информационной безопасности.

Результаты освоения факультативного курса

Личностные результаты:

- умение грамотно излагать свои мысли в устной и письменной речи;
- критичность мышления, умение распознавать достоверную информацию;
- представление об информатике как сфере человеческой деятельности, о ее значимости для развития цивилизации;
- активность при решении практических задач по основам информационной безопасности;
- умение контролировать процесс и результат учебной деятельности.

Метапредметные результаты:

- самостоятельно анализировать условия достижения цели на основе учета выделенных ориентиров действия в новом учебном материале;

- планировать пути достижения целей;
- уметь самостоятельно контролировать свое время и управлять им;
- сравнивать разные точки зрения, прежде чем принимать решения и выполнять практические действия;
- аргументировать свою точку зрения, спорить и отстаивать свою позицию не враждебным для оппонентов образом;
- задавать вопросы, необходимые для организации собственной деятельности и сотрудничества с партнером;
- осуществлять взаимный контроль и оказывать в сотрудничестве необходимую взаимопомощь;
- применять современные информационные технологии для коллективной, групповой и индивидуальной работы;
- осуществлять расширенный поиск информации с использованием ресурсов Интернета;
- владеть навыками ознакомительного, изучающего, усваивающего и поискового чтения;
- осуществлять выбор наиболее эффективных способов решения практических задач в сфере личной информационной безопасности в зависимости от конкретных условий;
- владеть навыками безопасного и целесообразного поведения при работе в информационном пространстве, соблюдать нормы информационной этики и права.

Предметные результаты:

- знать основные термины и понятия по проблематике информационной безопасности;
- знать основные положения нормативных документов в РФ, регламентирующих стратегию развития информационного общества России, защиту информации и баз данных, административную и уголовная ответственность в сфере информационной безопасности;
- знать разновидности угроз информационной безопасности государству и личности;
- знать принципы и методы организационной защиты информации;
- уметь выявлять и уничтожать компьютерные вирусы;
- уметь использовать методы защиты личного информационного пространства.

Содержание факультативного курса с указанием форм организации и видов деятельности

Наименование разделов, содержание	Формы организации	Виды деятельности
Раздел 1. Правовые основы информационной безопасности. Безопасность общения. Инструктаж по охране труда и организации автоматизарованного рабочего места обучающегося.	Вводное коллективное занятие, практическое	Проектирование собственного информационного пространства; самостоятельная работа с электронными образовательными ресурсами;

Информационное общество. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями на 18 марта 2019 года) Указ Президента Российской Федерации №203/2017 г. «О стратегии развития информационного общества в Российской Федерации до 2030 года» Распоряжение Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р «Концепция информационной безопасности детей» Административная и уголовная ответственность в сфере информационной безопасности. Порядок привлечения несовершеннолетних к гражданско-правовой ответственности за проступки в области информационной безопасности.	занятие за компьютером, групповой сетевой проект.	изучение нормативных документов по информационной безопасности; поиск информации в электронных базах и банках данных сети Интернет; отбор и сравнение материала из нескольких источников; подготовка и представление публичного выступления в виде групповой сетевой презентации.
Раздел 2. Киберпространство .«Безопасность устройств» Основные термины и понятия. Киберобщество. Виртуальная реальность. Кибермиры. Киберфизическая система. Кибермошенничество. Киберденьги. Киберкультура. Киберкнига. Киберискусство. Угрозы социальной инженерии. Новые профессии в киберобществе.	Занятия по углублению и совершенствова нию знаний, фронтальная, парная и индивидуальная работа, деловая игра, тестирование, практические работы за компьютером, индивидуальные проекты.	Работа с научно-популярной литературой, просмотр учебных видеороликов, самостоятельная работа с электронными образовательными ресурсами; выполнение заданий по разграничению понятий, тестирование по основным понятиям, систематизация учебного материала, деловая игра по презентации и обсуждению индивидуальных проектов, участие во Всероссийском уроке безопасности школьников в сети Интернет (28-31 октября 2019 года)
Раздел 3. Киберугрозы . Понятие нарушителя	Комбинированн ая форма	Слушание и анализ докладов одноклассников, отбор

информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация. Кибервойны. Киберпреступность. Запрещенные и нежелательные сайты.	организация занятий, групповая и парная работа, практические работы за компьютером, групповые проекты.	материала из нескольких источников, просмотр познавательных фильмов, видеоуроков, участие во Всероссийской акция «Час кода», проведение тематического урока информатики. (3-9 декабря 2019 года).
Раздел 4. Программно-аппаратные методы защиты информации. Безопасность информации. Лицензионное ПО и пиратство**,** свободное ПО. Обзор свободного антивирусного ПО и его возможности. Методы криптографии. Основные технологии построения защищенных систем. Модели безопасности для домашней информационной системы. Безопасность аккаунтов. Что такое аккаунт. Как взламывают аккаунты. Как защитить аккаунт. Что делать, если вас взломали. Личный контент в облаке и система его защиты. Безопасные он-лайн платежи. Настройки телефона, планшета для защиты от несанкционированного доступа.	Комбинированная форма организация занятий, групповая и парная работа, практические работы за компьютером, семинар, деловая игра, викторина, групповые проекты.	Систематизация знаний по программному обеспечению, самостоятельная работа с электронными образовательными ресурсами, применение методов клиптографии для решения практических задач, диагностика компьютера и устранение компьютерных вирусов, применение антивирусных программ для обеспечения стабильной работы технических средств, использование защищенных компьютерных систем, осуществлять выбор программного обеспечения и технических средств ИКТ для решения проблемы защиты информации, создание личного контента в облаке и организация его защиты, осуществление настройки телефона, планшета для защиты от несанкциони-рованного доступа, создание безопасный паролей**,** создание структурированных демонстрационных материалов с использованием возможностей современных программных средств, слушание и анализ презентаций проектов.

Тематическое планирование

№	Раздел	Общее кол-во часов	Форма организации занятий			
			практика			
			Деловая игра	Викторина	Практика за компьютером	Тестирование
1	Правовые основы информационной Безопасности. «Безопасность общения»	**4**			**2**	
2	Киберпространство. «Безопасность устройств»	**5**	**1**		**1**	**1**
3	Киберугрозы	**5**			**2**	
4	Программно-аппаратные методы защиты информации. Безопасность информации.	**20**	**1**	**1**	**12**	**1**
Итого		**34**	**2**	**1**	**16**	**2**
Итого		**34**	**21**			

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 327766045235508045123579633876966067016845890622

Владелец Стародубцева Антонина Михайловна

Действителен С 01.10.2023 по 30.09.2024