Муниципальное казенное образовательное учреждение
«Средняя общеобразовательная школа № 2 им. И.С.Унковского»

п.Воротынск Бабынинского района Калужской области

УТВЕРЖДЕНО
протоколом педагогического совета
от ____ _____ 20__ г. № ____
Директор школы
_____ Сорокин И.В.
подпись

Введено приказом № _____
от _____ _____ 20__ г.

РАБОЧАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
ПО КУРСУ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
ДЛЯ 7 КЛАССОВ

(VII класс – 1 час в неделю, 33 часа в год)

Составитель: Захарова Н.А., учитель информатики, I кв. категория

СОГЛАСОВАНО
Зам. директора _____
подпись

РАССМОТРЕНО
на заседании МО, протокол № __ от ___ августа 20___г.
Руководитель МО _____
подпись

Воротынск 2019 г.

Программа разработана на основе курса «Основы кибербезопасности» для 2-11 классов, авторы Тонких И.М., Комаров М.М., Ледовской В.И., Михайлов А.В., Москва, 2016 год

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

В соответствии со «Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на Перспективу до 2025 года», утвержденной распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, «Стратегией развития информационного общества в Российской Федерации», утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 и рядом других документов в числе многих других задач выделяются:

- обеспечение различных сфер экономики качественными информационными технологиями;
- обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Задача курса «Информационная безопасность» - совершенствование школьного образования и подготовки в сфере информационных технологий, а также популяризация профессий, связанных с информационными технологиями.

Цель изучения «Информационной безопасности» - дать общие представления о безопасности в информационном обществе и на этой основе сформировать понимание технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности.

Воспитательная цель курса – формирование на качественно новом уровне культуры умственного труда и взаимодействия с окружающими, ответственного отношения к вопросам безопасности жизнедеятельности

В рамках метапредметных результатов вопросы информационной безопасности обозначены:

- требование формирования навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права;
- умения использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;
- понимание основ правовых аспектов использования компьютерных программ и работы в Интернете.

.

СОДЕРЖАНИЕ КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

В соответствии с учебным планом на изучение информационной безопасности в 7 классе отводится 1 час в неделю, 33 часа в год.

Содержание программы соответствует обязательному минимуму содержания образования и имеет большую практическую направленность.

7 класс (33 часа)

Общие сведения о безопасности ПК и Интернета (6 часов)

Как работают мобильные устройства. Угрозы для мобильных устройств. Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр). Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации). Кто обеспечивает защиту киберпространства. Что такое геоинформационные системы. Глобальные информационные сети по стихийным бедствиям.

Информационная безопасность. Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные. Источники данных в Интернете: почта, сервисы обмена файлами и др. Хранение данных в Интернете. Возможности и проблемы социальных сетей. Безопасный профиль в социальных сетях. Составление сети контактов.

Техника безопасности и экология (6 часов)

Компьютеры и мобильные устройства в экстремальных условиях. Везде ли есть Интернет. ТБ при работе с мобильными устройствами. Первая помощь при проблемах в интернете (службы помощи). Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM) Комплекс упражнений при работе за компьютером. Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных,

монохромных мониторов. Проблемы Интернет- зависимости. Виды Интернет- зависимости. Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред. Киберкультура (массовая культура в сети) и личность. Психологическое воздействие информации на человека. Управление личностью через сеть

Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы (6 часов)

Как распространяются вирусы. Источники и причины заражения. Скорая компьютерная помощь. Признаки заражения компьютера. Что такое антивирусная защита. Как лечить компьютер. Защита мобильных устройств. Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные. Защита файлов. Что такое право доступа. Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети. Защита файлов. Права пользователей. Защита при загрузке и выключении компьютера. Безопасность при скачивании файлов. Безопасность при просмотре фильмов онлайн.

Мошеннические действия в Интернете. Киберпреступления (6 часов)

Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС. Прослушивание разговоров. Определение местоположения телефона. Утечка и обнародование личных данных. Подбор и перехват паролей. Взломы аккаунтов в социальных сетях. Виды мошенничества в Интернете. Фишинг (фарминг). Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею.

Сетевой этикет. Психология и сеть (6 часов)

Что такое личные данные. Все, что выложено в Интернет, может стать известно всем. «Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам. Анонимность в сети. Что такое этикет. Виды этикета (личный, деловой, письменный, дискусси онный и пр.). Различия этикета в разных странах. Как появился нетикет, что это такое. Общие правила сетевого этикета. Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений). Этика дискуссий. Взаимное уважение при интернет-общении. Этикет и безопасность. Эмоции в сети, их выражение. Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться. Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер- моббинг, троллинг, буллицид. Если вы стали жертвой компьютерной агрессии: службы помощи.

Правовые аспекты защиты киберпространства (3 часа)

Защита прав потребителей при использовании услуг Интернет. Защита прав потребителей услуг провайдера. Государственная политика в области кибербезопасности. Войны нашего времени. Что такое кибервойна. Что такое информация. Право на информацию в Конституции. Почему государство защищает информацию. Защита государства и защита киберпространства.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Наименование раздела	Количество часов	Сроки прохождения материала
1	Общие сведения о безопасности ПК и Интернета	6	03.09.2019-08.10.2019
2	Техника безопасности и экология	6	15.10.2019-03.12.2019
3	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы	6	10.12.2019-28.01.2020
4	Мошеннические действия в Интернете. Киберпреступления	6	04.02.2020-18.03.2020
5	Сетевой этикет. Психология и сеть	6	01.04.2020-06.05.2020
6	Правовые аспекты защиты киберпространства	3	13.05.2020-27.05.2020