Краснодарский край Каневской район ст. Челбасская
Муниципальное общеобразовательное учреждение
средняя общеобразовательная школа №26
имени Заслуженного учителя школы РФ А. Е. Дашутина
муниципального образования Каневской район

УТВЕРЖДЕНО

Бузан Елена Григорьевна

Подписано цифровой подписью: Бузан Елена Григорьевна

решением педагогического совета
от 31.08.2023 г протокол № 1
Председатель _____ Бузан Е. Г.

РАБОЧАЯ ПРОГРАММА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Объединение «Кибербезопасность»
(наименование)

__2 года__
(срок реализации программы)

10-11 класс
(возраст обучающихся)

Федорец А.Н.
(Ф.И.О. учителя, составителя)

1. Результаты обучения

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».

Необходимо совершенствовать современную профессиональную подготовку учителей информатики и преподавателей дисциплин в сфере информационных технологий», а значит, и в сфере кибербезопасности. Киберугрозы существуют везде, где применяются информационные технологии, следовательно, преподаватель любой дисциплины может в профессиональной деятельности столкнуться и со спамом, и с вирусами, и со взломом компьютера и с многими другими проблемами, на которые нужно не только оперативно реагировать, но и насколько возможно уметь предотвращать их появление, а значит, постоянно упоминать в контексте урока различные аспекты организации информационной безопасности. Преподаватель должен иметь представление о современном уровне развития вычислительной техники, информационный сетей, технологий коммуникации и навигации. С учетом роста числа угроз информационной деятельности и стремительного развития информационных технологий представляется необходимым включить в ФГОСы соответствующие требования, что позволило бы органически дополнить образовательный процесс новыми модулями без рассогласования с имеющимися учебными планами. В число требований к результатам подготовки учащихся необходимо включить не только «удовлетворение познавательных интересов, поиск дополнительной информации», знание «технических устройств (в том числе компьютеров)», умение «искать информацию с применением правил поиска (построения запросов) в базах данных, компьютерных сетях, пользоваться персональным компьютером и его периферийным оборудованием; следовать требованиям техники безопасности, гигиены, эргономики и ресурсосбережения при работе со средствами информационных и коммуникационных технологий», но и знание основ кибербезопасности, умения соблюдать требования кибербезопасности в практической деятельности и организовывать безопасность личного информационного пространства.

2. Содержание программы

Тема №1. Общие сведения о безопасности Интернета (3 часа)

Категории персональных данных. Биометрические персональные данные. Безопасный профиль в социальных сетях. Составляет сети, контактов. Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности. Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации. Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, без законные тиражирование (воспроизведение). Безопасный серфин . Безопасные ресурсы для поиска.

Тема №2. Интернет - зависимость (2 часа)

ЗОЖ и компьютер. Деструктивная информация в Интернет как ее избежать. Психологическое воздействие информации на человека. Управление личностью через сеть. Интернет и компьютер зависимость (аддикция). Критерии зависимости точки зрения психологов (приоритетность, изменения, настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость. Типы интернет - зависимости (пристрастие к работе с компьютером, зависимость от сетевого общения, сексуальные зависимости).

Тема №3. Виртуальное общение (6 часов) Как устроен интернет. Как работают мобильные устройства. Угрозы для мобильных устройств. Защита персональных данных, почему она нужна.

Тема №4. Киберкультура (5 часов)

Виды интернет - мошенничества (письма, реклама, охота за личными данными и т. п.). Фишинг (фарминг). Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды. Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса. Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС. Прослушивание разговоров. Определение местоположения телефона. Азартные игры. Онлайн - казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею. Технологии манипулирования в Интернете. Техника безопасности при интернет - общении.

Тема №5 . Вирусы (11 часов)

Вирусы человека и компьютера, цели компьютерных вирусов. Типы вирусов. Отличия вирусов и закладок. Как распространяются вирусы. Что такое антивирусная защита . Как лечить компьютер .Антивирусные программы для ПК: сканеры , ревизоры и др. Выявление неизвестных вирусов. Защита мобильных устройств. Безопасность при скачивании файлов. Защита программ и данных от несанкционированного копирования.

Организационные, юридические, программные и программно - аппаратные меры защиты. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Методы защиты фото и видеоматериалов от копирования в сети. Проверка подлинности (аутентификация) в Интернете. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.

Предотвращение несанкционированного доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей.

Тема №6 Сетевой этикет. (7 часов)

Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах, как появился этикет, что это такое. Сетевой этикет. Общие правила сетевого этикета. Этика дискуссий. Взаимное уважение при интернет - общении. Этикет и безопасность. Эмоции в сети, их выражение. Примеры этических нарушений. Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). термины сетевого этикета: оверквотинг, флейм. флуд. оффтопик,смайлики и др. Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг. троллинг. буллицид. Если вы стали жертвой компьютерной агрессии: службы помощи личное .общение и общение в группе - чем они отличаются (чаты, форумы, службы мгновенных сообщений)

Учебно-тематический план

Название раздела	Теория	Практика
1. Общие сведения о безопасности ПК и Интернета - 3 часа	2	1
2. Интернет-зависимость - 2 часа	1	1
3. Виртуальное общение - 6 часов	4	2
4. Киберкультура - 5 часов	2	3
5. Вирусы-11 часов	6	5
6. Сетевой этикет - 7часов	4	3
Итого:	19	15