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

решением педагогического совета
от 30 августа 2022 года протокол № 1
Председатель _____ Бузан Е. Г.

РАБОЧАЯ ПРОГРАММА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

комплексная
(тип программы)

Объединение «Кибербезопасность»
(наименование)

по социальному направлению

2 года
(срок реализации программы)

10 - 11 классы
(возраст обучающихся)

Пстеян А. А.
(Ф.И.О. учителя, составителя)

1. Результаты обучения

Данная программа составлена на основе курса «Основы кибербезопасности» для общеобразовательных организаций авторов Тонких И.М., Комарова М.М., Ледовского В.И., Михайлова А.В., переработана и модифицирована.

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.

Безопасность в информационном обществе является одним из основных направлений фундаментальных исследований в области информационных технологий.

Компьютерные технологии применяются при изучении практически всех школьных дисциплин уже с младших классов. Киберугрозы существуют везде, где применяются информационные технологии.

Государство считает необходимым расширение объема преподавания информационных технологий в общеобразовательных организациях. В качестве одной из организационных мер в обеспечении кибербезопасности определена разработка и внедрение в учебный процесс образовательных организаций разного уровня курса по информационной безопасности, включающего модули по обеспечению кибербезопасности, либо дополнение имеющихся курсов упомянутыми модулями. Школьная программа должна соответствовать этим целям, поэтому представляется актуальным реализация программы внеурочной деятельности «Основы кибербезопасности».

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

Цель изучения «Кибербезопасности» - 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.

Цель программы – создание условий для формирования у учащихся цифровой культуры личности с необходимыми навыками и присущими ценностями, взглядами,

ориентациями, установками, мотивами деятельности и поведения для обеспечения безопасной и развивающей жизнедеятельности учащегося в сети «Интернет».

Для достижения поставленной цели решаются следующие задачи:

- Формирование у учащихся цифровой и информационной культуры;
- Воспитание у учащихся нравственности и культуры взаимоотношения с людьми на основе общечеловеческих ценностей в сети «Интернет»;
- Утверждение в сознании и чувствах учащихся правильных моделей поведения, ценностей, взглядов и убеждений для успешной жизнедеятельности учащегося в сети «Интернет»;
- Углубление знаний учебных дисциплин «Информатика», «ОБЖ» и «Обществознание» в процессе обучения в рамках программы;
- Интеллектуальное развитие учащихся, формирование творческих и прикладных качеств мышления;
- Развитие интереса к различным сферам информационных технологий;
- Совершенствование навыков самообразования, всестороннего развития и социализации;
- Обучение поиску и отбору информации, её интерпретации и применимости;
- Развитие логического мышления, умений обобщения и конкретизации, анализа и синтеза;
- Воспитание умения трудиться, самостоятельности, ответственности и творческого отношения к учёбе;

Обучающие:

- Сформировать систему знаний в сфере обществознания, информационных технологий и основ безопасности жизнедеятельности;
- Обучить элементам системного мышления использовать инструменты активизации мышления;
- Отработка навыков и умений для безопасного и полезного использования информационных технологий: сравнение информации, критический анализ, выделение главных мыслей и грамотное изложение, а также восприятия и усвоения информации из сети «Интернет».

Развивающие:

- Развить интеллектуальные и социальные способности обучающихся;
- Развить навыки сетевого общения и коммуникации в сети «Интернет», поиска и работы с информацией, обеспечения безопасности цифровых устройств и аккаунтов и осуществления сетевых покупок;
- Развить деловые и гражданские качества, такие как самостоятельность, ответственность, активность и аккуратность;
- Сформировать потребности в самопознании и саморазвитии.

Воспитательные:

- Воспитать культуру общения и поведения в сетевом пространстве;
- Воспитать целеустремлённость личности;
- Воспитать толерантную и культурную личность;
- Воспитать правильный образ гражданина.

Курс «Кибербезопасность» структурирован по модульному принципу. Он включает в себя 7 модулей:

- *Общие сведения о безопасности ПК и Интернета*
- *Техника безопасности и экология*
- *Проблемы Интернет-зависимости*
- *Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы*
- *Мошеннические действия в Интернете. Киберпреступления*

- *Сетевой этикет. Психология и сеть*
- *Правовые аспекты защиты киберпространства*

Данный курс реализуется в рамках социального направления внеурочной деятельности и рассчитан на 1 час в неделю в 10 классе, 1 час в неделю в 11 классе (68 часов).

2. Содержание программы

10 класс

Модуль 1. Общие сведения о безопасности ПК и Интернета (5 часов).

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

Модуль 2. Техника безопасности и экология (2 часа).

1. Комплекс упражнений при работе за компьютером.
2. Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов.

Модуль 3. Проблемы Интернет-зависимости (3 часа).

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

Модуль 4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы (16 часов).

1. Защита файлов. Права пользователей.
2. Защита при загрузке и выключении компьютера.
3. Безопасность при скачивании файлов.
4. Безопасность при просмотре фильмов онлайн.
5. Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты.
6. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы.
7. Методы защиты фото и видеоматериалов от копирования в сети.
8. Защита от копирования контента сайта.
9. Как развивались вирусы.
10. Могут ли вирусы воздействовать на аппаратуру ПК.
11. Как вирусы воздействуют на файлы.
12. Проверка на наличие вирусов. Сканеры и др.
13. Может ли вирус воздействовать на рабочий стол.
14. Источники заражения ПК.
15. Антивирусное ПО, виды и назначение.
16. Методы защиты от вирусов. Как распознаются вирусы.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления (4 часа).

1. Утечка и обнародование личных данных.
2. Подбор и перехват паролей. Взломы аккаунтов в социальных сетях.
3. Виды мошенничества в Интернете. Фишинг (фарминг).

4. Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею.

Модуль 6. Сетевой этикет. Психология и сеть (1 час).

1. Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид.

Модуль 7. Правовые аспекты защиты киберпространства (3 часа).

1. Защита прав потребителей при использовании услуг Интернет.
2. Защита прав потребителей услуг провайдера.
3. Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

11 класс

Модуль 1. Общие сведения о безопасности ПК и Интернета (11 часов).

1. Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности.
2. Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации.
3. Что такое защищенная информационная среда. Защита каналов передачи данных, средства предотвращения утечки информации, защита информации от НСД (антивирусная защита, средства контроля защищенности, средства обнаружения и предупреждения атак), средства аутентификации.
4. Организационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения информации, средства резервного копирования и восстановления.
5. Требования к безопасности информации: сохранение целостности, конфиденциальности и доступности. Определения по ГОСТ РВ 51987-2002 «Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем. Общие положения».
6. Признаки нарушения целостности программ и данных. Способы нарушения целостности информации. Признаки и способы нарушения конфиденциальности. Признаки и способы нарушения доступности информации.
7. Безопасность мобильных устройств в информационных системах. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты).
8. Угрозы безопасности в сетях WiFi. Методы защиты сетей WiFi.
9. Угрозы информации (техногенные, случайные и преднамеренные; природные). Неосторожность пользователя как одна из угроз для информационной безопасности.
10. Меры кибербезопасности для конечных пользователей. Использование рекомендованных версий операционных систем и приложений, использование антивирусных средств, настройка веб-браузеров, блокировка скриптов, использование фильтров фишинга, межсетевых экранов. Автоматическое обновление ПО.
11. Киберугрозы Интернета (кибервойны, манипулирование людьми, зависимость, вирусные атаки, отсутствие приватности).

Модуль 2. Техника безопасности и экология (3 часа).

1. Кибератаки на инфраструктуру.
2. Компьютер в режиме труда и отдыха. Информационная перегрузка.
3. Влияние компьютера на репродуктивную систему.

Модуль 3. Проблемы Интернет-зависимости (2 часа).

1. Интернет - и компьютерная зависимость (аддикция). Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость.
2. Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости).

Модуль 4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы (7 часов).

1. Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.). Методы защиты.
2. Проверка подлинности (аутентификация) в Интернете.
3. Меры безопасности для пользователя WiFi. Настройка безопасности.
4. Вирусы для мобильных устройств (мобильные банкеры и др.).
5. Настройка компьютера для безопасной работы.
6. Ошибки пользователя (установка нескольких антивирусов, установка слишком большого числа программ, отсутствие резервного копирования и т.п.).
7. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления (7 часов).

1. Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы.
2. Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники.
3. Мошеннические действия в сети. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды.
4. Что такое электронный кошелек – удобства и проблемы безопасности. «Обменники» для электронных денег.
5. Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса.
6. Платные предложения работы. Платный просмотр видеоматериалов.
7. Технологии манипулирования в Интернете.

Модуль 6. Сетевой этикет. Психология и сеть (1 час).

1. Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Сетевой этикет. Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др.

Модуль 7. Правовые аспекты защиты киберпространства (3 часа).

1. Как расследуются преступления в сети.
2. Ответственность за интернет-мошенничество.
3. Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

3. Учебно-тематический план

№ п/п	Наименование модулей		Кол-во часов		
		10 класс(теория)	10 класс(практика)	11 класс(теория)	11 класс(практика)
1	Общие сведения о безопасности ПК и Интернета	2	3	4	7
2	Техника безопасности и экология.	1	1	1	2
3	Проблемы Интернет-зависимости	1	2	1	1

4	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы	8	8	3	4
5	Мошеннические действия в Интернете. Киберпреступления	2	2	3	4
6	Сетевой этикет. Психология и сеть	1		1	
7	Правовые аспекты защиты киберпространства	2	1	1	2
	Всего часов:	**17**	**17**	**14**	**20**

СОГЛАСОВАНО
Протокол №___заседание МО
учителей математики, физики и информатики

Руководитель МО_____ Федорец А.Н.

СОГЛАСОВАНО
Заместитель директора по ВР
_____ Дюмина Ю.Э.
подпись Ф.И.О.
30.08.2022 года.