ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА С. ВАСИЛЬЕВКА ИМЕНИ ГЕРОЯ СОВЕТСКОГО СОЮЗА Е. А. НИКОНОВА МУНИЦИПАЛЬНОГО РАЙОНА СТАВРОПОЛЬСКИЙ САМАРСКОЙ ОБЛАСТИ

УТВЕРЖДАЮ
к использованию в образовательном учреждении
«__1___» сентября 2021_ года
директор ГБОУ СОШ с. Васильевка
_____/С.В.Хопова/

ПРОГРАММА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

«Информационная безопасность»

Для обучающихся (8-х классов)

Направление внеурочной деятельности:

Научно-познавательное

I. Пояснительная записка

Данная программа составлена на основе курса «Информационная безопасность» 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 2014-2022 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 «Информационная безопасность».

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

II. Общая характеристика курса

Курс «Информационная безопасность» 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

III. Описание места учебного предмета в учебном плане.

Данный курс реализуется в рамках социального направления внеурочной деятельности и рассчитан на 1 час в неделю (34 часа).

IV. Содержание учебного предмета

8 класс

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

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.

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

Комплекс упражнений при работе за компьютером.

Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов.

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

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.

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

Защита файлов. Права пользователей.

Защита при загрузке и выключении компьютера.

Безопасность при скачивании файлов.

Безопасность при просмотре фильмов онлайн.

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. Неперемещаемые программы.

Методы защиты фото и видеоматериалов от копирования в сети.

Защита от копирования контента сайта.

Как развивались вирусы.

Могут ли вирусы воздействовать на аппаратуру ПК.

Как вирусы воздействуют на файлы.

Проверка на наличие вирусов. Сканеры и др.

Может ли вирус воздействовать на рабочий стол.

Источники заражения ПК.

Антивирусное ПО, виды и назначение.

Методы защиты от вирусов. Как распознаются вирусы.

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

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.

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

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

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

Защита прав потребителей при использовании услуг Интернет.

Защита прав потребителей услуг провайдера.

Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

V. Планируемые результаты изучения курса

Предметные:

1. Сформированы знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет;
2. Сформированы умения соблюдать нормы информационной этики;
3. Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

Метапредметные:

1. Развиваются компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных технологий;
2. Развиваются умения анализировать и систематизировать имеющуюся информацию;
3. Развиваются познавательная и творческая активность в безопасном использовании информационных и коммуникационных технологий.

Личностные:

1. Вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;
2. Формируются и развиваются нравственные, этические, патриотические качества личности;
3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

VI. Тематическое планирование

№ п/п	Наименование модулей	Кол-во часов
		8 класс
1	Общие сведения о безопасности ПК и Интернета	5
2	Техника безопасности и экология.	2
3	Проблемы Интернет-зависимости	3
4	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы	16
5	Мошеннические действия в Интернете. Киберпреступления	4
6	Сетевой этикет. Психология и сеть	1
7	Правовые аспекты защиты киберпространства	3
	Всего часов:	**34**

VII. Учебно-методическое и материально-технического обеспечения образовательного процесса

Методические материалы

Тонких И.М., Комаров М.М., Ледовской В.И., Михайлов А.В. Основы кибербезопасности, Москва, 2016

Портал Международного квеста по цифровой грамотности www.Сетевичок.рф
https://toipkro.ru/content/files/documents/podrazdeleniya/ordo/ciber%20bezopasnost.pdf

Экранно-звуковые пособия
Видеофильмы по основным разделам курса
Презентации по тематике курса

Технические средства обучения
Ноутбук
Телевизор.
Мультимедиапроектор.
Экран навесной.
Средства телекоммуникации (электронная почта, выход в Интернет).

Календарно-тематическое планирование 8 класс (34 часа)

№ урока	Тема	Кол-во часов
	Общие сведения о безопасности ПК и Интернета	**5**
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.	
	Техника безопасности и экология.	**2**
6	Комплекс упражнений при работе за компьютером.	
7	Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов.	
	Проблемы Интернет-зависимости.	**3**
8	Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред.	
9	Киберкультура (массовая культура в сети) и личность.	
10	Психологическое воздействие информации на человека. Управление личностью через сеть.	
	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	**16**
11	Защита файлов. Права пользователей.	
12	Защита при загрузке и выключении компьютера.	
13	Безопасность при скачивании файлов.	
14	Безопасность при просмотре фильмов онлайн.	
15	Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты.	
16	Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы.	[i]
17	Методы защиты фото и видеоматериалов от копирования в сети.	
18	Защита от копирования контента сайта.	
19	Как развивались вирусы.	
20	Могут ли вирусы воздействовать на аппаратуру ПК.	
21	Как вирусы воздействуют на файлы.	
22	Проверка на наличие вирусов. Сканеры и др.	
23	Может ли вирус воздействовать на рабочий стол.	
24	Источники заражения ПК.	

[i] ? Уроки проводимые с применением оборудования Центра «Точка Роста» отмечены цветом.

25	Антивирусное ПО, виды и назначение.	
26	Методы защиты от вирусов. Как распознаются вирусы.	
	Мошеннические действия в Интернете. Киберпреступления.	**4**
27	Утечка и обнародование личных данных.	
28	Подбор и перехват паролей. Взломы аккаунтов в социальных сетях.	
29	Виды мошенничества в Интернете. Фишинг (фарминг).	
30	Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею.	
	Сетевой этикет. Психология и сеть.	**1**
31	Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид.	
	Правовые аспекты защиты киберпространства.	**3**
32	Защита прав потребителей при использовании услуг Интернет.	
33	Защита прав потребителей услуг провайдера.	
34	Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».	

C=RU, O=ГБОУ СОШ с. Васильевка,
CN=Хопова С.В.,
E=vasilev_sch@samara.edu.ru
00f6128d334d2e4d72
2021.09.01 10:06:55+04'00'