C=RU, OU=и.о. директора школы, O=ГБОУ СОШ им.М.П.Крылина с.Кабановка, CN=Таинкина Людмила Анатольевна, E=tainkina.lludmila@yandex.ru
ГБОУ СОШ им. М. П. Крылина с. Кабановка
2022.09.14 16:21:39

Государственное бюджетное общеобразовательное учреждение среднего общего образования Самарской области средняя общеобразовательная школа имени Героя Советского Союза Михаила Петровича Крыгина села Кабановка муниципального района Кинель-Черкасский Самарской области

УТВЕРЖДЕНО:
И.о. директора школы:_____/Л.А. Таинкина/

Приказ № 49-ОД от 29.08.2022 г.

РАБОЧАЯ ПРОГРАММА
внеурочной деятельности

_____Информационная безопасность_____
(полное наименование)

_____9 класс_____
(классы)

_____духовно-нравственное_____
(направление)

_____2022-2023 учебный год_____
(срок реализации)

СОСТАВИТЕЛИ (РАЗРАБОТЧИКИ)

Должность: учитель математики и информатики
Ф.И.О. Золотарева В.В.

«ПРОВЕРЕНО»
Учитель, ответственный за ВР:
_____Павлова С.А.
Дата: 26.08.2022 г

Аннотация к рабочей программе по внеурочной деятельности «Информационная безопасность»

Нормативная база программы:	Рабочая программа внеурочной деятельности рекомендована Координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019)
Дата утверждения:	2908.2022 г
Общее количество часов:	34 часа
Уровень реализации:	базовый
Срок реализации:	2022-2023
Автор(ы) рабочей программы:	Золотарева В.В.

Рабочая программа реализуется в рамках духовно — нравственного развития личности обучающихся. Рабочая программа составлена на 34 часа в год, в неделю - 1час; занятия проводятся 1 раз в неделю по 40 минут в течение года. Форма обучения – очная, кружковая

Характеристика личностных, метапредметных и предметных результатов освоения учебного курса (Модуль 1)

Предметные:

Выпускник научится:

- анализировать доменные имена компьютеров и адреса документов в интернете;
- безопасно использовать средства коммуникации, безопасно вести и применять способы самозащиты при попытке мошенничества, безопасно использовать ресурсы интернета.

Выпускник овладеет:

- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов ит.п.

Выпускник получит возможность овладеть:

- основами соблюдения норм информационной этики и права;
- основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;
- использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет- ресурсы и другие базы данных.

Метапредметные.

Регулятивные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- идентифицировать собственные проблемы и определять главную проблему;
- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ставить цель деятельности на основе определенной проблемы и существующивозможностей;
- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- составлять план решения проблемы (выполнения проекта, проведения исследования);
- описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- выделять явление из общего ряда других явлений;
- определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
- строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
- излагать полученную информацию, интерпретируя ее в контексте решае- мой задачи;
- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;

- критически оценивать содержание и формутекста;
- определять необходимые ключевые поисковые слова и запросы.

Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- строить позитивные отношения в процессе учебной и познавательной деятельности;
- критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
- договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
- делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его.
- целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных язы- ков в соответствии с условиями коммуникации;
- использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, со- здание презентаций и др.;
- использовать информацию с учетом этических и правовых норм;
- создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правил а информационной безопасности.

Личностные.

- осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
- готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
- освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах исообществах;
- сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Содержание учебного курса (Модуль 1).

№ п/п	Тема	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
Тема 1. «Безопасность общения»			
1	Общение в социальных сетях и мессенджерах	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.
2	С кем безопасно общаться в интернете	Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.
3	Пароли для аккаунтов социальных сетей	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить.
4	Безопасный вход в аккаунты	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.
5	Настройки конфиденциальности в социальных сетях	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.

6	Публикация информациив социальныхсетях	Персональные данные. Публикация личной информации.	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.
7	Кибербуллинг	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
8	Публичные аккаунты	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
9	Фишинг	Фишинг как мошеннический прием. Популярные варианты распространения фишинга.Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу.
10	Выполнение и защита индивидуальных и групповых проектов		Самостоятельная работа.
Тема 2. «Безопасность устройств»			
1	Что такое вредоносный код	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.
2	Распространение вредоносного кода	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка.Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов наустройствах.	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационнойбезопасностиобъектов.

3	Методы защиты от вредоносных программ	Способы защиты устройств от вредоносного кода. Антивирусные программы характеристики. Правила защиты от вредоносных кодов.	Изучает виды антивирусных программ и правила их установки.
4	Распространение вредоносного кода для мобильных устройств	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.
5.	Выполнение и защита индивидуальных и групповыхпроектов		Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.
Тема 3 «Безопасность информации»			
1	Социальная инженерия: распознать иизбежать	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.
2	Ложная информация в Интернете	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Определяет возможные источники необходимыхсведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам.
			Анализируетиоценивает достоверность информации.

3	Безопасность при использовании платежных карт в Интернете	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете.
4	Беспроводная технология связи	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Используя различную информацию, определяетпонятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.
5	Резервное копирование данных	Безопасность личной информации. Создание резервных копий на различных устройствах.	Создает резервные копии.
6	Основы государственной политики в области формирования культуры информационной безопасности	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.	Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации; - отражающего правовые аспекты защиты киберпространства.
7	Выполнение и защита индивидуальных и групповых проектов		
8	Повторение, волонтерская практика, резерв		

Тематическое планирование

№ п/п	Название раздела	Содержание раздела	Количество часов

1	«Безопасность общения»	**Тема 1. Общение в социальных сетях и мессенджерах.** Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	1
2		**Тема 2. С кем безопасно общаться в интернете.** Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	1
3		**Тема 3. Пароли для аккаунтов социальных сетей.** Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	1
4		**Тема 4. Безопасный вход в аккаунты.** Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	1
5		**Тема 5. Настройки конфиденциальности в социальных сетях.** Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	1
6		**Тема 6. Публикация информации в социальных сетях.** Персональные данные. Публикация личной информации.	1
7		**Тема 7. Кибербуллинг.** Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	1
8		**Тема 8. Публичные аккаунты.** Настройки приватности публичных страниц. Правила ведения публич- ных страниц. Овершеринг.	1
9		**Тема 9. Фишинг.** Фишинг как мошеннический прием. Популярные варианты распространения фишинга.Отличие настоящих и фишинговыхсайтов. Как защититься от фишеров в социальных сетях и мессенджерах. Выполнение и защита индивидуальных и групповых проектов. 3 часа	5
10	«Безопасность устройств»	**Тема 1. Что такое вредоносный код.** Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	1
11		**Тема 2. Распространение вредоносного кода.** Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия приобнаружении вредоносных кодов на устройствах.	1

12		**Тема 3. Методы защиты от вредоносных программ.** Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	2
13		**Тема 4. Распространение вредоносного кода для мобильных устройств.** Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства. Выполнение и защита индивидуальных и групповых проектов. 3 часа	4
14	«Безопасность информации»	**Тема 1. Социальная инженерия: распознать и избежать.** Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	1
15		**Тема 2. Ложная информация в Интернете.** Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	1
16		**Тема 3. Безопасность при использовании платежных карт в Интернете.** Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	1
17		**Тема 4. Беспроводная технология связи.** Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	1
18		**Тема 5. Резервное копирование данных.** Безопасность личной информации. Создание резервных копий на различных устройствах.	1
19		**Тема 6. Основы государственной политики в области формирования культуры информационной безопасности.** Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности. Выполнение и защита индивидуальных и групповых проектов. Повторение. Волонтерская практика. 3 часа	5

Список источников:

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум/А.В.Бабаш,Е.К.Баранова,Ю.Н.Мельников.–М.:КноРус,2019.–432с
2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014. – 182с.
3. ГромовЮ.Ю.Информационнаябезопасностьизащитаинформации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384с.
4. Дети в информационном обществе // http://detionline.com/journal/about
5. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.:ЮНИТИ-ДАНА,2016.–239с.
6. ЗапечниковС.В.Информационнаябезопасностьоткрытыхсистем.В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558с.
7. Защита детей by Kaspersky //https://kids.kaspersky.ru/
8. Кузнецова А.В. Искусственный интеллект и информационная безопасностьобщества/А.В.Кузнецова,С.И.Самыгин,М.В.Радионов.–М.:Ру- сайнс, 2017. – 64с.
9. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.:Просвещение, 2019.–80с.
10. Основы кибербезопасности. // https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa
11. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.
12. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности // Студенческий: электрон. научн. журн. 2019. №22(66)
13. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144с.