государственное бюджетное общеобразовательное учреждение

средняя общеобразовательная школа с. Среднее Аверкино

муниципального района Похвистневский Самарской области

«Проверена»

Заместитель директора по УВР

ГБОУ СОШ с. Среднее Аверкино

_____/В.В.Кириллова/

____30.08.2023 г_____

«Утверждена»

приказом директора школы

ГБОУ СОШ с. Среднее Аверкино

№ 178 – од от _30.08.2023 г__

_____/В.Н.Ромаданов/

РАБОЧАЯ ПРОГРАММА ПО ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

«Информационная безопасность»

Класс: 5

Направление: общеинтеллектуальное

Вид программы: Интеллектуальный марафон

Составитель: Щенева Юлия Валерьевна

C=RU, O=ГБОУ СОШ с. Среднее Аверкино, CN=Ромаданов В.Н., E=sraverkino@yandex.ru
00af4e116fd9904d55
2023.08.30 08:35:39+03'00'

«Рассмотрено» на заседании методического объединения естественнонаучного цикла

протокол № _1_ от _29.08.2023 г__

руководитель МО

_____/Кириллова В. В. /

1. Планируемые результаты освоения учебного предмета: «Информационная безопасность»

Предметные результаты

В результате изучения учебного предмета «Информационная безопасность» на уровне среднего общего образования:

Выпускник на базовом уровне 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.
- идентифицировать собственные проблемы и определять главную проблему;
- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- 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;
- основам соблюдения норм информационной этики и права;
- основам 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.

2. Содержание предмета 8 класс

Раздел 1. История возникновения Интернета

Понятия Интернет-угроз. Изменения границ допустимого в контексте цифрового образа жизни. Изменения нормативных моделей развития и здоровья детей и подростков.

Раздел 2. Информационная безопасность

Зачем это нужно? Понятие периметра безопасности. Обеспечение эмоционально-психологического периметра безопасности в соответствии с возрастными особенностями ребенка. Баланс ценностей развития и ценностей безопасности.

Раздел 3. Угрозы информационной безопасности

Атаки, связанные с компьютерной, социальной инженерией. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах. Груминг, кибербуллинг. Чему мы должны научить ребенка для профилактики насилия в Сети? Фишинг. Обращение с деньгами в сети Интернет. Детская пластиковая карта: быть или не быть?

Раздел 4. Контентные риски

Настройка и безопасное использование смартфона или планшета. Семейный доступ.

Тематическое планирование

8 класс (34часа)

№ темы	Название и программное содержание темы	Количество часов
Раздел 1. *История возникновения Интернета (5 ч)*		
1	Понятия Интернет- угроз.	1
2	Цифровой образ жизни. Изменение границ допустимого в контексте	2
3	Изменения нормативных моделей развития и здоровья детей и подростков	2
Раздел 2. *Цифровая гигиена (8 ч)*		
4	Цифровая гигиена**:** зачем это нужно?	2
5	Понятие периметра безопасности	2
6	Обеспечение эмоционально-психологического периметра безопасности в соответствии с возрастными особенностями ребенка	2
7	Баланс ценностей развития и ценностей безопасности.	2
Раздел 3. *Угрозы информационной безопасности (18 ч)*		
8	Атаки, связанные с компьютерной инженерией	2
9	Способы выявления наличия вредоносных кодов на устройствах.	2
10	Действия при обнаружении вредоносных кодов на устройствах.	2
11	Атаки, связанные с социальной инженерией.	2
12	Груминг.	2
13	Кибербуллинг	2
14	Чему мы должны научить ребенка для профилактики насилия в Сети?	1
15	Фишинг	2
16	Обращение с деньгами в сети Интернет.	2
17	Детская пластиковая карта: быть или не быть?	1
Раздел 4. *Контентные риски(2 ч)*		
	Настройка и безопасное использование смартфона или планшета. Зачет.	1
	Семейный доступ.	1
ИТОГО:		34

Список использованной литературы:

1. Основы кибербезопасности: учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М.: Дрофа, 2019. — 238, [1] с. — (Российский учебник).

2. Баранова Е.К., Бабаш А.В. Основы информационной безопасности: учебник / Е.К. Баранова, А.В. Бабаш. — М.: РИОР: ИНФРА-М, 2019. — 202 с. — (Среднее про - фессиональное образование)

3. Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2018, 474 с.

4. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы: учеб.пособие для общеобразоват. организаций / М.С. Наместникова. – М.: Просвещение, 2019. – 79 с.: ил. – (Внеурочная деятельность).

5. Цветкова, М.С. Информационная безопасность. Кибербезопасность . 7–9 классы: учебное пособие /М.С. Цветкова, И.Ю. Хлобыстова. — 2-е изд., пересмотр. — М.: БИНОМ. Лаборатория знаний, 2020 — 64 с.: ил.

6. Шаньгин В.Ф. Информационная безопасность и защита информации. / Шаньгин В.Ф. – ДМК-Пресс, 2017 – 702 с.

Электронные (цифровые) образовательные ресурсы.

https://olimp.edsoo.ru

https://edu.skysmart.ru

https://www.yaklass.ru/

https://uchi.ru

https://урок.рф

https://education.yandex.ru

https://resh.edu.ru