

муниципальное бюджетное общеобразовательное учреждение
«Школа № 99»
городского округа Самара

ПРОВЕРЕНО

Заместитель директора по ВР

Петрова Д.В.

(подпись)

«30» августа 2022 г

УТВЕРЖДАЮ

Директор МБОУ Школы № 99

Мергалиева Б.А.

(подпись)

«31» августа 2022 г

РАБОЧАЯ ПРОГРАММА
внеурочной деятельности
«Информационная безопасность»

На I и II полугодие 2022/ 2023 учебного года

Классы: 8-9

Учитель: Ещенко Ольга Николаевна

(Фамилия, Имя, Отчество)

Программа составлена учителем физической культуры Ещенко Ольгой Николаевной
(название и авторы программы)

Рекомендованной (утвержденной) МО учителей математики МБОУ «Школа № 99»
г. о. Самара протокол №1 от (30. 08. 2022 г.)

(кем рекомендована, утверждена, когда)

Форма организации: кружок

Учебники и учебные пособия:

- Автор М.С.Наместникова
- Название Информационная безопасность, или На расстоянии одного вируса. 7-9 классы/
- Издательство М.: Просвещение,
- Год издания 2019

Рассмотрен на заседании МО

математика

(название методического объединения)

Протокол № 1 от « 30 » августа 20 22 г.

Председатель МО

Селиверстова Т.Н.

(Фамилия, Имя, Отчество)

(Подпись)

Пояснительная записка

Программа курса «Информационная безопасность» адресована родителям обучающихся 1–11 классов с использованием материалов Федерального государственного образовательного стандарта основного общего образования, примерной рабочей программы учебного курса «Цифровая гигиена» для основной школы и линии учебников М.С.Наместникова Информационная безопасность, или На расстоянии одного вируса. 7-9 классы/ М.: Просвещение, 2019.

Основная цель изучения курса «Информационная безопасность» – формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Данный курс предполагает организацию работы с родителями обучающихся в рамках культурно-просветительской и профилактической деятельности педагогического коллектива школы.

При работе с родителями важнейшей задачей является преодоление «цифрового разрыва» и обучение родителей правильной оценке своих возможностей в помощи детям в Интернете – возможностей, которые достаточно велики.

Методы реализации курса: репродуктивный – (беседа, вопросы); проблемный; частично-поисковый – (творческие задания); объяснительно-иллюстративный.

Составители курса предполагают, что родители с бóльшей готовностью включатся в программу развития цифровой гигиены, предлагающую им общение, совместный поиск, развивающие игры, просмотр отрывков из познавательных, научно-популярных фильмов, видеороликов, обсуждение ситуативных иллюстраций, творческая работа, работа в группах и т.п. Вместе с тем формами проведения мероприятий для родителей также могут являться: лектории, выступления на родительских собраниях, микро-обучение на основе технологий он-лайн обучения, геймификация, создание чек-листов, совместное обучение, совместные родительско-детские проекты и пр.

**Календарно-тематическое планирование курса занятий
«Информационная безопасность»**

| | | |
|---|---|--|
| 1 | Тема 1. История возникновения Интернета. Понятия Интернет-угроз. Изменения границ допустимого в контексте цифрового образа жизни | |
| 2 | Тема 2. Изменения нормативных моделей развития и здоровья детей и подростков. | |
| 3 | Тема 3. Цифровая гигиена: зачем это нужно? Понятие периметра безопасности. Обеспечение эмоционально-психологического периметра безопасности в соответствии с возрастными особенностями ребенка. Баланс ценностей развития и ценностей безопасности. | |
| 4 | Тема 4. Угрозы информационной безопасности: атаки, связанные с компьютерной инженерией. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах. | |
| 5 | Тема 5. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Груминг, кибербуллинг. Чему мы должны научить ребёнка для профилактики насилия в Сети? | |
| 6 | Тема 6. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Фишинг. Обращение с деньгами в сети Интернет. Детская пластиковая карта: быть или не быть? | |
| 7 | Тема 7. Контентные риски. Настройка и безопасное использование смартфона или планшета. Семейный доступ. | |
| 8 | Тема 8. Пособия и обучающие программы по формированию навыков цифровой гигиены. | |

Литература

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с
2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014. – 182 с.
3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.
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. – 239 с.
6. Запечников С.В. Информационная безопасность открытых систем. 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. – 558 с.
7. Защита детей by Kaspersky // <https://kids.kaspersky.ru/>
8. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Ру-сайтс, 2017. – 64 с.
9. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.
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. – 144 с.