ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ ОСНОВНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА с. СЕВРЮКАЕВО МУНИЦИПАЛЬНОГО РАЙОНА СТАВРОПОЛЬСКИЙ САМАРСКОЙ ОБЛАСТИ

Рассмотрено:	Согласовано:	Утверждаю:
на заседании Методического совета _____/. В.В.Львов Протокол № _1_ «26 » августа 2024г.	зам. директора по УВР _____/В.В.Львов «26 » августа 2024г.	И.о.директора ГБОУ ООШ с. Севрюкаево _____/А.В. Ярославлев Приказ № 54-од от «26» августа 2024г.

Рабочая программа по внеурочной деятельности «Цифровая гигиена»

Общеинтеллектуальное направление

Класс: 7
Срок реализации программы: 1 год
Составитель: Лапшова М.А.., учитель информатики

ЭП
C=RU, OU=и.о.диретора, O=ГБОУ ООШ с.Севрюкаево, CN=А_В_Ярославлев, E=shkola.sevryukaevo@yandex.ru
00e187a962c67a68a9
2024-10-29 11:07:54

Севрюкаево 2024

Рабочая программа внеурочной деятельности «Цифровая гигиена» для 7 класса составлена с учётом требований Федерального закона "Об образовании в РФ" от 29.12.2012 N 273-ФЗ; ФГОС ООО (Приказ №1897 от 17.12.2010г.) на основе примерной рабочей программы учебного курса «Цифровая гигиена», рекомендованной координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол №27 от 21.08.2019).
Срок реализации рабочей программы - 1 год, количество часов в год — 34ч.
При составлении рабочей программы учтены основные идеи и положения Программы развития и формирования универсальных учебных действий для основного общего образования.

Планируемые результаты освоения курса внеурочной деятельности.

Предметные:

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.

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 существующихвозможностей;
выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы длярешения 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.

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 решаемой задачи; самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и
применять способ проверки достоверности информации;
критически оценивать содержание и форму текста;
определять необходимые ключевые поисковые слова и запросы.
Коммуникативные универсальные учебные действия.
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 языков 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, создание презентаций и др.;
использовать информацию с учетом этических и правовых норм;
создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила 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 и сообществах;
сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно- телекоммуникационной среде.

Содержание курса внеурочной деятельности «Цифровая гигиена» с указанием форм организации и видов деятельности.
7 класс – 1 час в неделю/ 34 часа в год.

Раздел 1. «Безопасность общения»
Тема 1. Общение в социальных сетях и мессенджерах. 1 час.

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальныхсетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. 1 час.

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей. 1 час.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использованиефункции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.

Настройки приватности и конфиденциальности в разных социальных сетях. Приватностьи конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. 1 час.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 1 час.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. 1 час.

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг. 2 часа.

Фишинг как мошеннический приём. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 час.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 час.

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 на устройствах.

Тема 3. Методы защиты от вредоносных программ. 2 час.

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.

Расширение вредоносных кодов для мобильных устройств. Правила безопасности приустановке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 1 час.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 1 час.

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.

Транзакции и связанные с ними риски. Правила совершения онлайн поупок. Безопасностьбанковских сервисов.

Тема 4. Беспроводная технология связи. 1 час.

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы впубличных сетях.

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культурыинформационной безопасности. 2 час.

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. 3 часа. Повторение. Волонтерская практика. 3 часа.

Тематическое планирование

№	Разделы и темы	Кол-во часов
Раздел 1. «Безопасность общения»		
1.	Общение в социальных сетях и мессенджерах	1
2.	С кем безопасно общаться в интернете	1
3.	Пароли для аккаунтов социальных сетей	1
4.	Безопасный вход в аккаунты	1
5.	Настройки конфиденциальности в социальных сетях	1
6.	Публикация информации в социальных сетях	1
7.	Кибербуллинг	1
8.	Публичные аккаунты	1
9-10.	Фишинг	2
11-13.	Выполнение и защита индивидуальных и групповых проектов	3
Раздел 2. «Безопасность устройств»		
14.	Что такое вредоносный код	1
15.	Распространение вредоносного кода	1
16-17.	Методы защиты от вредоносных программ	2

18.	Распространение вредоносного кода для мобильных устройств	1
19-21.	Выполнение и защита индивидуальных и групповых проектов	3
Раздел 3 «Безопасность информации»		
22.	Социальная инженерия: распознать и избежать	1
23.	Ложная информация в Интернете	1
24.	Безопасность при использовании платежных карт в Интернете	1
25.	Беспроводная технология связи	1
26.	Резервное копирование данных	1
27-28.	Основы государственной политики в области формирования культуры информационной безопасности	2
29-31.	Выполнение и защита индивидуальных и групповых проектов	3
32-34.	Повторение, волонтерская практика, резерв Итоговое мероприятие «Лестница успеха»	3

Приложение 1

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.: Русайнс, 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