Муниципальное бюджетное общеобразовательное учреждение
городского округа Тольятти «Лицей № 76 имени В.Н. Полякова»

ПРИНЯТА
на заседании
Педагогического совета
Протокол №1 от 27.08.2025 г.

УТВЕРЖДЕНА
приказом директора
МБУ «Лицей № 76»
№ 120-од от 27.08.2025 г.

О="МБУ ""Лицей №76""", CN="Коняхина Юлия Станиславовна, директор", E=school76@edu.tgl.ru
00 d8 58 4b 0b 04 ac 37 64
2025.11.12 13:01:13+04'00'

РАБОЧАЯ ПРОГРАММА

КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

«Цифроваягигиена»

Общеинтеллектуальноенаправление

Класс:7

Срокреализациипрограммы:1год

Составитель/ли:Лукоянова А.С.,учительинформатики

Тольятти
2025

Рабочая программа внеурочной деятельности «Цифровая гигиена» для 7 класса составлена с учетом требований Федерального закона "Об образовании в РФ" от 29.12.2012N273-ФЗ;ФГОСООО;Федеральнойобразовательнойпрограммыосновногообщегообразования(приказМинпросвещенияРоссии №370 от 18.05.2023), ООПОООМБУ«Лицей № 76»; на основе примерной рабочей программы учебного курса «Цифровая гигиена», рекомендованной координационным советом учебно-методическихобъединений в системе общего образования Самарской области (протокол №27 от 21.08.2019).

Срокреализациирабочейпрограммы«Цифровая гигиена» - 1 год, количество часов в год — 34ч.Программа ориентирована на обеспечение индивидуальных потребностей обучающихся и направлена на достижение планируемых результатов федеральных основных образовательных программ начального общего, основного общего и среднего общего образования с учётом выбора участниками образовательных отношений курсов внеурочной деятельности.

В Учебном плане МБУ «Лицей №76» на прохождение курса в 7 классах отводится по одному часу в неделю. ***Реализация программы - 2025-2026 уч. году.***

Рабочаяпрограммакурса внеурочной деятельности «Цифровая гигиена» определяетсодержаниедеятельностисучетомособенностейобразовательнойполитикиМБУ«Лицей№76»,образовательныхпотребностейизапросовобучающихся.При составлениирабочей программы учтены основные идеи и положения Программы развития и формирования универсальных учебных действий для основного общего образования.

Планируемыерезультатыосвоениякурсавнеурочной деятельности.

Предметные:

анализироватьдоменныеименакомпьютеровиадресадокументоввинтернете; безопасно использовать средства коммуникации,

безопасновестиилиприменятьспособысамозащитыприпопыткемошенничества, безопасно использовать ресурсы интернета.

Метапредметные.

Регулятивныеуниверсальныеучебныедействия.

Врезультатеосвоенияучебногокурсаобучающийся сможет:

идентифицироватьсобственныепроблемыиопределятьглавнуюпроблему;

выдвигатьверсиирешенияпроблемы,формулироватьгипотезы,предвосхищать конечный результат;

ставитьцельдеятельностинаосновеопределеннойпроблемыисуществующих возможностей;

выбиратьизпредложенных вариантов исамостоятельноискатьсредства/ресурсы для решения задачи/достижения цели;

составлять план решения проблемы (выполнения проекта, проведения исследования); описыватьсвойопыт,оформляяегодляпередачидругимлюдямввидетехнологии

решенияпрактическихзадачопределенногокласса;

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;

приниматьрешениевучебнойситуациии нестизанего ответственность.

Познавательныеуниверсальныеучебныедействия.

выделятьявлениеизобщегорядадругихявлений;

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; самостоятельноуказыватьнаинформацию,нуждающуюсявпроверке,предлагатьи

применятьспособпроверкидостоверностиинформации;

критическиоцениватьсодержаниеиформутекста;

определятьнеобходимыеключевыепоисковыесловаи запросы.

Коммуникативныеуниверсальныеучебныедействия.

строить позитивные отношения в процессе учебной и познавательной деятельности; критическиотноситьсяксобственномумнению,сдостоинствомпризнавать

ошибочностьсвоегомнения(еслионотаково)икорректироватьего;

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 своихмыслейсредствамиестественныхиформальныхязыковвсоответствииусловиями коммуникации;

использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) длярешенияинформационныхикоммуникационныхучебныхзадач,втомчисле:вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;

использоватьинформациюсучетомэтическихиправовыхнорм;

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.

Содержаниекурсавнеурочнойдеятельности«Цифроваягигиена» с указанием форм организации и видов деятельности.
7класс–1 часвнеделю/ 34часав год.

Раздел1.«Безопасностьобщения»

Тема1.Общениевсоциальныхсетяхимессенджерах.1час.

Социальнаясеть.Историясоциальныхсетей.Мессенджеры.Назначениесоциальныхсетей и мессенджеров. Пользовательский контент.

Тема2.Скембезопаснообщатьсявинтернете.1час.

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

Тема3.Паролидляаккаунтовсоциальныхсетей.1час.

Сложныепароли.Онлайнгенераторы паролей.Правилахраненияпаролей.Использование функции браузера по запоминанию паролей.

Тема4.Безопасныйвходваккаунты.1час.

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

Тема5.Настройкиконфиденциальностивсоциальныхсетях.1час.

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

Тема6.Публикацияинформациивсоциальныхсетях.1час.
Персональныеданные.Публикацияличнойинформации.
Тема7.Кибербуллинг.1час.
Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать?Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.
Тема8.Публичныеаккаунты.1час.
Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.
Тема9.Фишинг.2часа.
Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.
Выполнениеизащитаиндивидуальныхигрупповыхпроектов.3часа.

Раздел 2. «Безопасность устройств»
Тема1.Чтотакоевредоносныйкод.1час.
Видывредоносныхкодов.Возможностиидеструктивныефункциивредоносных кодов.
Тема2.Распространениевредоносногокода.1час.
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.
Тема3.Методызащитыотвредоносныхпрограмм.2час.
Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.
Тема4.Распространениевредоносногокодадлямобильныхустройств.1час.
Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.Выполнениеизащитаиндивидуальныхигрупповыхпроектов.3часа.

Раздел 3 «Безопасность информации»
Тема1.Социальнаяинженерия:распознатьиизбежать.1час.
Приемысоциальнойинженерии.Правилабезопасностиприviртуальныхконтактах.
Тема2.ЛожнаяинформациявИнтернете.1час.
Цифровоепространствокак площадкасамопрезентации,экспериментированияи освоения различных социальных ролей. Фейковые новости. Поддельные страницы.
Тема3.Безопасность прииспользованииплатежныхкартвИнтернете.1час.
Транзакции и связанные с ними риски. Правила совершения онлайн поупок. Безопасность банковских сервисов.
Тема4.Беспроводнаятехнологиясвязи.1час.
УязвимостьWi-Fi-соединений.Публичныеинепубличныесети.Правилаработыв публичных сетях.
Тема5.Резервноекопированиеданных.1час.
Безопасность личной информации. Создание резервных копий на различных устройствах.
Тема6.Основыгосударственнойполитикивобластиформированиякультуры информационной 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.
Выполнениеизащитаиндивидуальныхигрупповыхпроектов.3часа.
Повторение. Волонтерская практика. 3 часа.

Тематическоепланированиекурсавнеурочнойдеятельности«Цифроваягигиена»

№	Тема	Кол-вочасов
Тема1.«Безопасность общения»		
1.	Общениевсоциальныхсетяхи мессенджерах	1
2.	Скембезопаснообщатьсяв интернете	1
3.	Паролидляаккаунтовсоциальныхсетей	1
4.	Безопасныйвходваккаунты	1
5.	Настройкиконфиденциальностивсоциальныхсетях	1
6.	Публикацияинформациивсоциальныхсетях	1
7.	Кибербуллинг	1
8.	Публичныеаккаунты	1
9-10.	Фишинг	2
11-13.	Выполнениеизащитаиндивидуальныхигрупповыхпроектов	3
Тема2.«Безопасность устройств»		
14.	Чтотакоевредоносныйкод	1
15.	Распространениевредоносногокода	1
16-17.	Методызащитыотвредоносныхпрограмм	2
18.	Распространениевредоносногокодадлямобильныхустройств	1
19-21.	Выполнениеизащитаиндивидуальныхигрупповыхпроектов	3
Тема3«Безопасность информации»		
22.	Социальнаяинженерия:распознатьиизбежать	1
23.	Ложнаяинформацияв Интернете	1
24.	БезопасностьприиспользованииплатежныхкартвИнтернете	1
25.	Беспроводнаятехнологиясвязи	1
26.	Резервноекопированиеданных	1
27-28.	Основыгосударственнойполитикивобластиформирования культуры информационной безопасности	2
29-31.	Выполнениеизащитаиндивидуальныхигрупповыхпроектов	3
32-34.	Повторение,волонтерскаяпрактика,резерв Итоговое мероприятие «Лестница успеха»	3

Литература:

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с

2. ГромовЮ.Ю. Информационная безопасность и защита информации: Учебноепособие/ Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.

3. Детивинформационномобществе//http://detionline.com/journal/about

4. 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.

5. ЗащитадетейbyKaspersky//https://kids.kaspersky.ru/

6. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017. – 64 с.

7. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.

8. Основы кибербезопасности. // https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa

9. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности // Студенческий: электрон.научн. журн. 2019. № 22(66)