МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Государственное бюджетное общеобразовательное учреждение Самарской области

средняя общеобразовательная школа с. Переволоки

муниципального района Безенчукский Самарской области

ГБОУ СОШ с.Переволоки

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
на заседании	Куратор УР	директор
ШМО ГБОУ СОШ с. Переволоки	_____	_____
_____	Разина В.В.	Бурма Е.А.
Протокол №1 от «30» августа 2024 г.	.	Приказ № от «30» августа 2024 г.

РАБОЧАЯ ПРОГРАММА

ПО ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

«Информационная безопасность»

для обучающихся 7 класса

с. Переволоки 2024

Рабочая программа внеурочной деятельности учебного курса «Информационная безопасность» (далее – Программа) предназначена для обучающихся 7 классов и рассчитана на 1 год обучения.

Программа включает три раздела:

• «Планируемые результаты освоения курса внеурочной деятельности»;

• «Содержание курса внеурочной деятельности»;

• «Тематическое планирование».

Программа разработана в соответствии с:

• Рабочей программой учебного курса «Цифровая гигиена», рекомендованной Координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол№ 27 от 21.08.2019)

• Основной образовательной программой основного общего образования ГБОУ СОШ с. Переволоки.

Планируемые результаты освоения курса внеурочной деятельности

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.

Метапредметные

Регулятивные универсальные учебные действия:

- 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;

- 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 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.

Предметные:

- анализировать доменные и компьютерные адреса документов в интернете;
- безопасно использовать средства коммуникации,
- безопасно вести и применять способы самозащиты при попытке мошенничества,
- безопасно использовать ресурсы интернета.
- владеть приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.
- владеть основами соблюдения норм информационной этики и права;
- владеть 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.

Содержание курса внеурочной деятельности

Содержание программы учебного курса соответствует темам основной образовательной программы основного общего образования по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Учебный курс «Информационная безопасность» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей.

Основными **целями** изучения учебного курса «Информационная безопасность» являются:

- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;
- формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

- сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием

цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);

- создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;
- сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
- сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Каждый раздел учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

За счет часов, предусмотренных для повторения материала (4 часа), возможно проведение занятий для учащихся 4-6 классов. Эти занятия в качестве волонтерской практики могут быть проведены учащимися, освоившими программу. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн занятия, подготовленные в ходе выполнения учебных заданий по основным темам курса.

7класс(34ч.)

Раздел 1. «Безопасность общения»

Тема1.Общениевсоциальныхсетяхимессенджерах.1час.

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей 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.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. 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.1 час.

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

Тема6.Публикацияинформациивсоциальныхсетях.1час.

Персональные данные. Публикация личной информации.

Тема7.Кибербуллинг.1 час.

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. Какзащититься от фишеров в социальных сетях и мессенджерах.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

<u>Раздел 2. «Безопасность устройств»</u>

Тема1.Чтотакоевредоносныйкод.1час.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных 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.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 при установке приложений на мобильные устройства.

Выполнениеизащитаиндивидуальныхигрупповыхпроектов.3 часа.

<u>Раздел3«Безопасностьинформации»</u>

Тема1.Социальная инженерия: распознать и избежать.1час.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема2.Ложная информация в Интернете.1час.

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

Тема3.Безопасностьприиспользовании платежныхкартвИнтернете.1 час.

Транзакциии связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема4.Беспроводнаятехнологиясвязи.1 час.

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

Тема5.Резервноекопированиеданных.1 час.

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.3 часа.

Повторение.Волонтерскаяпрактика.3часа.

Формы организации:

- традиционный урок (коллективная и групповая формы работы)
- тренинги (в классической форме и липокейс-методу)
- дистанционное обучение (видеоролики, почтовые рассылки)
- диспуты
- проекты
- общественно-полезные практики

Виды деятельности

- Познавательная
- Проблемно-ценностное общение
- Техническое творчество
- Проектная деятельность

Оценивание результативности освоения обучающимися программы внеурочной деятельности «Информационная безопасность» осуществляется с помощью тестирования. (см. Приложение).

Критерии оценки результатов тестов:

- 80–100%-высокий уровень освоения программы;
- 60-80%-уровень выше среднего;
- 50-60%-средний уровень;
- 30-50%-уровень ниже среднего
- меньше30%-низкий уровень.

Тематическое планирование

Согласно плану внеурочной деятельности ГБОУ ООШ № 9 г. Новокуйбышевска на реализацию рабочей программы учебного курса «Информационная безопасность», выделено по 1 часу в неделю в 7-ом, всего 34 часа в год.

№ п/п	Тема	Количество часов
	Тема1.«Безопасностьобщения»	
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	Фишинг	2
10	Выполнение и защита индивидуальных и групповых проектов	3
	Тема2.«Безопасностьустройств»	
1	Что такое вредоносный код	1
2	Распространение вредоносного кода	1
3	Методы защиты от вредоносных программ	2
4	Распространение вредоносного кода для мобильных устройств	1
5	Выполнение и защита индивидуальных и групповых проектов	3
	Тема3«Безопасностьинформации»	
1	Социальная инженерия: распознать и избежать	1
2	Ложная информация в Интернете	1
3	Безопасность при использовании платежных карт Интернете	1
4	Беспроводная технология связи	1
5	Резервное копирование данных	1
6	Основы государственной политики в области формирования Культуры информационной безопасности	2
7	Выполнение и защита индивидуальных и групповых проектов	3
8	Повторение	2
9	Волонтерская практика	1
	Итого	34

Приложение

Тест1

Раздел1«Безопасностьобщения»

1) Аккаунт социальной сети-это…

a) Графическое представление пользователя
b) онлайн-сервис или веб-сайт
c) учетная запись, личная страница пользователя

2) Что такое социальная сеть?

a) Программа для загрузки интернет-страниц
b) интернет-страница или веб-сайт, позволяющий общаться и обмениваться информацией
c) учетная запись

3) Установить соответствие между функциями браузера и их описанием

1) История посещения страниц
2) Сохранение паролей
3) Управление всплывающими окнами
4) Управление информацией о местоположении
5) автозаполнение

a) упрощает доступ к регулярно посещаемым сайтам за счет автоматического ввода
b) автоматическая блокировка всплывающих окон
c) возврат на посещенную страницу или восстановление события
d) использование данных о местоположении для вывода ближайших запрашиваемых мест
e) доступ к регулярно посещаемым сайтам за счет автоматического заполнения учетных данных

4) Что необходимо для входа в аккаунт?

a) инверсия
b) логин
c) скриншот
d) аватар
e) пароль

5) Выберете информацию, которую безопасно размещать на своей странице:

a) хобби

b) паспортные данные
c) местоположение
d) любимые книги
e) номер школы
f) домашний адрес
g) любимые места в городе

6) Отметьте простые пароли для использования в учетной записи:
a) sqwertb
b) Tdscg12_5v
c) MyAccc.ert
d) uipot
e) eve.try
f) Reper1987
g) Qwasd.13%7

7) Что такое двухфакторная аутентификация?

8) Кибербуллинг–это...
a) Навязчивое внимание к человеку со стороны другого человека
b) угрозы, травля, оскорбления в интернете
c) доступ в режиме реального времени к пользовательскому контенту

9) Какие настройки конфиденциальности следует установить, чтобы обезопасить себя от мошенников?
a) приватность подарков
b) приватность персональных данных
c) приватность списка друзей
d) приватность местоположения
e) приватность фотографий
f) приватность аудиозаписей

Тест2

Раздел2«Безопасностьустройств»

1) Соотнесите названия вредоносных кодов с их описанием:
1) вирус
2) троян
3) червь
4) руткиты
5) бэкдор
6) загрузчик

a) часть кода, используемая для загрузки и установки вредоносной программы
b) самовоспроизводящийся вредоносный код
c) вредоносная программа, которая устанавливается на компьютере отдельным файлом и распространяется через сеть Интернет
d) вредоносная программа, которая может блокировать, изменять, повреждать, удалять, шифровать данные на устройстве
e) вредоносная программа, которую после активации трудно обнаружить на устройстве
f) программа для получения доступа к данным и удаленного управления устройством

2) Что такое расширение?
a) последовательность букв после точки в названии файла для обозначенияего формата
b) алгоритм для автоматизации каких-то процессов
c) комплекс программ, предназначенный для управления файлами

3) Как распространяются вредоносные программы?
a) При посещении популярных сайтов
b) С помощью вложенных в электронные письма файлов
c) При авторизации в социальной сети
d) С помощью файлообменников и торрентов
e) При переходе по ссылке для подтверждения регистрации
f) При использовании зараженной интернет страницы

4) Отметьте истинные высказывания
a) Трояны и вирусы распространяются самостоятельно
b) Трояны распространяются самостоятельно, а вирусы распространяют люди
c) Трояны распространяют люди, а вирусы распространяются самостоятельно
d) Трояны и вирусы распространяют люди
e) Черви распространяются самостоятельно

f) Черви распространяют люди

5) Отметьте виды программ, которые всегда вредоносны:
a) утилиты
b) макросы
c) троян
d) руткиты
e) софт
f) бэкдор
g)скрипт

6) Что такое спам?
a) Массовые незапрашиваемые рассылки
b) Вредоносный код
c) вредоносная программа

7) На какие параметры следует обращать внимание, приобретая антивирусные программы?

8) Что такое операционная система(ОС)?
a) игровая платформа
b) комплекс программ, предназначенный для управления ресурсами технического устройства
c) вспомогательная программа, созданная для выполнения типовых задач

9) Когда получен спам-mail с приложенным файлом, следует:
a) Прочитать приложение, если оно не содержит ничего ценного–удалить
b) Сохранить приложение в папке «Спам», выяснить IP-адрес генератора спама
c) Удалить письмо с приложением, не раскрывая (не читая) его

10) Чтобы предотвратить заражение вирусами необходимо:
a) Регулярное обновление операционной системы
b) Проверка всех ссылок и файлов, полученных по электронной почте
c) Установка только лицензионной версии программного обеспечения
d) Отказ от перехода по ссылкам из всплывающих окон
e) Установка на компьютер сразу нескольких средств защиты
f) загрузка программного обеспечения только с официальных сайтов разработчиков

Тест3

Раздел3«Безопасностьинформации»

1) Объясните следующие понятия:
a) Фейковый сайт
b) Фейковый аккаунт
c) Фейковые новости
d) Фейковая кредитная карта

2) Что такое СМИ?
a) Распространение ложной информации
b) Процесс несанкционированной активности в инфраструктуре, атакуемой системы
c) Совокупность органов публичной передачи информации с помощью технических средств

3) Соедините понятия с их определениями:
1) гаджет
2) патч
3) интерфейс
4) VPN (Virtual private network)
5) WEP (wired equivalent privacy)
6) роутер

a) виртуальная частная сеть, используемая для доступа к корпоративной сети
b) прибор, позволяющий настроить сеть Интернет между подключенными к нему устройствами
c) портативное техническое устройство
d) алгоритм для обеспечения безопасности сети Wi-Fi
e) набор инструментов, предназначенный для взаимодействия человека и технического устройства
f) исправления и дополнения программного кода

4) Для безопасной работы с Wi-Fi в публичном месте необходимо:
a) По возможности использовать мобильный интернет
b) Выбирать сеть, название которой совпадает с названием заведения
c) Обновлять программные обеспечения из публичных сетей
d) Уточнять у сотрудников сеть, которой лучше воспользоваться
e) Использовать VPN
f) Нажимать продолжить, если появилось объявление об ошибке сертификата
g) Подключаться к сетям без авторизации

5) Какое шифрование, предназначенное для защиты сети, легковзломать?

a) WEP
b) WPA
c) WPA2

6) Резервное копирование позволяет...
a) Обезопасить хранимую информацию от повреждений и выхода из строя
b) Защищает информацию от вредоносных программ и вирусов
c) Позволяет восстановить ценную информацию, поврежденную
или удаленную на устройстве

7) Критерии, обеспечивающие безопасность, при использовании интернет-магазинов и совершении онлайн-платежей
a) Обновление операционной системы
b) обновление браузера
c) компьютер близких родственников
d) цена на товар значительно ниже среднерыночной цены
e) антивирусная защита устройства
f) большое количество исключительно хвалебных отзывов

Ответы на тесты

Тест1

1)c ; **2)**b; **3)**1-c,2-e,3-b,4-d,5-a; **4)**b, e; **5)**a, d,g; **6)**a, d,e ;

7) логин, пароль и подтверждение через(минимум2) смс, голосовой вызов, мобильное приложение, наличие устройств: usb-токен, смарт-карта

8) b; **9)**b,d, e

Тест2

1) 1-b,2-d,3-c,4-e,5-f,6-a; **2)**a; **3)**b,d,e,f; **4)**c,e; **5)**c,d,f; **6)**a;

7) (минимум 5) платность/бесплатность, уровень детектирования (обнаружения вредоносных программ), уровень ложных срабатываний, разнообразие функций (умение работать с вредоносным кодом, фишингом,
спамом, предупреждение об обновлениях операционной системы), влияние на скорость работы компьютера, ресурсоемкость, русский язык (русский интерфейс)

8) b; **9)**c; **10)**a,c,d, f

Тест3

1) (фейковый—поддельный, фальсифицированный, лживый, фальшивый)

Фейковый сайт-фальсифицированный сайт, копия страницы известного сайта

Фейковый аккаунт—аккаунт с недостоверной информацией (имя,контакты, фотографии)

Фейковые новости—фальшивые новости

Фейковая кредитная карта—банковская карта, оформленная на несуществующего человека

2) c ; **3)**1-c,2-f,3-e,4-a,5-d,6-b; **4)**a,d,e; **5)**a; **6)**c; **7)**a,b,e