основная общеобразовательная школа № 12 имени М.В. Яковенко
пос. Шмидта городского округа Новокуйбышевск Самарской области
(ГБОУ ООШ № 12 пос. Шмидта г.о. Новокуйбышевск)
446219, Россия, Самарская обл., г.о. Новокуйбышевск, пос. Шмидта, ул. Школьная, д. 4
телефон 884635 31768, e-mail sch12_nkb@samara.edu.ru

«РАССМОТРЕНА»
Председатель ШМС
_____ А.Ю. Колесник
протокол № 1
от «26» августа 2021 г.

«СОГЛАСОВАНА»
Педагог, выполняющий
обязанности заместителя
директора по ВР
ГБОУ ООШ № 12
пос. Шмидта
г.о. Новокуйбышевск
_____ Т.Н. Петрова

«УТВЕРЖДАЮ»
Директор
ГБОУ ООШ № 12
пос. Шмидта
г.о. Новокуйбышевск
_____ Е.Б. Забоева
приказ № 74-од
от 26.08. 2021 г.

РАБОЧАЯ ПРОГРАММА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
ДЛЯ 7 КЛАССА

Елена Борисовна Забоева

Подписан: Елена Борисовна Забоева
DN: C=RU, O=ГБОУ ООШ №. 12 пос. Шмидта г.о. Новокуйбышевск, CN=" Елена Борисовна Забоева ", E=sch12_nkb@samara.edu.ru
Основание: Я являюсь автором этого документа
Местоположение: место подписания
Дата: 2021.12.28 14:41:06+04'00'
Foxit PDF Reader Версия: 11.1.0

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ

Предметные:

Выпускник научится:

- Анализировать доменные имена компьютеров и адреса документов в интернете;
- Безопасно использовать средства коммуникации;
- Безопасно вести применять способы самозащиты при попытке мошенничества;
- Безопасно использовать ресурсы интернета.

Выпускник овладеет:

- Приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Выпускник получит возможность овладеть:

- Основами соблюдения норм информационной этики и права;
- Основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасностижизнедеятельности;
- Использовать для решения коммуникативных задач в области безопасностижизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

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 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 изменяющейсяситуациии/илипри отсутствии планируемогорезультата;
- 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.

В результате освоения учебного курса обучающийся сможет:

- 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 частныхявленийк общимзакономерностям;
- 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.

В результате освоения учебного курса обучающийся сможет:

- 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 длярешенияучебных ипрактических задачспомощью средств ИКТ;
- выбирать, строить и использовать адекватную информационную модель для передачисвоихмыслейсредствамиестественныхиформальныхязыковвсоответствииусловиямикоммуникации;
- 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 универсальные учебные действия.

- осознанное, уважительное и доброжелательное отношение к окружающим людям вреальном 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 вгруппахи сообществах;
- сформированность понимания ценности безопасного образа жизни;
- интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

СОДЕРЖАНИЕ

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

Каждый раздел учебного курса завершается выполнением проверочного теста.

1. «Безопасность общения». 13 часов

Общение в социальных сетях и мессенджерах. 1 час. Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

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.

Пароли для аккаунтов социальных сетей. 1час. Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Безопасный вход в аккаунты. 1 час. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Настройки конфиденциальности в социальных сетях. 1 час. Настройки приватности конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Публикация информации в социальных сетях. 1 час. Персональные данные. Публикация личной информации.

Кибербуллинг. 1 час. Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Публичные аккаунты. 1 час. Настройки приватности публичных страниц. Правилаведенияпубличных страниц. Овершеринг.

Фишинг. 2 часа. Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Самостоятельная работа. 3 часа.

2. «Безопасность устройств». 8 часов.

Что такое вредоносный код. 1 час. Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

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.

Методы защиты от вредоносных программ. 2 час. Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Распространение вредоносного кода для мобильных устройств. 1 час. Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Самостоятельная работа. 3 часа.

3. «Безопасность информации». 10 часов.

Социальная инженерия: распознать и избежать. 1 час. Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Ложная информация в Интернете. 1 час. Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Безопасность при использовании платежных карт в Интернете. 1 час.

Транзакциии связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковскихсервисов.

Беспроводная технология связи. 1 час. Уязвимость Wi-Fi-соединений. Публичные инепубличныесети. Правилаработы впубличныхсетях.

Резервное копирование данных. 1 час. Безопасность личной информации. Создание резервных копий на различных устройствах.

Основыгосударственнойполитикивобластиформированиякультурыинформационнойбезопасности. 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.

Самостоятельная работа. 3 часа.

Повторение. Резерв. 3 часа.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Тема	Количество часов		
		теория	практика	всего
	Общение в социальных сетях и мессенджерах			
1	Правила общения в социальных сетях	1	1	2
2	Безопасность в мессенджерах	1	1	2
3	Личная информация в сети	0,5	0,5	1
	С кем безопасно общаться в интернете			
4	Безопасное общение в сети	1	1	2
	Методы защиты от вредоносных программ			
5	Антивирусы	2		2
6	Виды вредоносных ПО	2		2
	Безопасный вход в аккаунты			
7	Защита социальных сетей	2	1	3
	Настройки конфиденциальности в социальных сетях			
8	Конфиденциальность в сети	1	1	2
	Публикация информации в социальных сетях			
9	Публикации в сети	1	1	2
	Кибербуллинг			
10	Что такое кибербуллинг?	2		2
11	Как не поддаться агрессии в сети	1	1	2
	Публичные аккаунты		2	2
12	Ведение аккаунтов в сети		2	2
	Фишинг			
13	Фишинговые сайты	2	2	4
	Выполнение и защита индивидуальных и групповых проектов			
14	Итоговый проект	2	2	4
ИТОГО		**18,5**	**15,5**	**34**