МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Министерство образования и науки Республики Башкортостан

Городского округа город Уфа

МАОУ Школа № 108

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
на заседании ШМО учителей математики	Заместитель директора по ВР	И.о. директора
_____	_____	_____
Мостипан М.Н	Галлямов И.Р.	Галлямов И.Р.
Протокол №1 от «30» 08 2023 г.	Приказ №301 от «31» 08 2023 г.	Приказ №301 от «31» 08 2023 г.

РАБОЧАЯ ПРОГРАММА

по внеурочной деятельности
учебного предмета «Безопасность детей в сети Интернет»

для обучающихся 8–9 классов

г. Уфа 2023-2024

I. Планируемые результаты освоения учебного предмета

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 ценности безопасного образа жизни;

– интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные результаты

В ходе изучения учебного курса обучающиеся усовершенствуют опыт проектной деятельности и навыки работы с информацией, в том числе в текстовом, табличном виде, виде диаграмм и пр.

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;

– формулировать учебные задачи как шаги достижения поставленной цели деятельности;

– обосновывать целевые ориентиры и приоритеты ссылками на ценности, указывая и обосновывая логическую последовательность шагов;

– определять необходимые действие(я) в соответствии с учебной и познавательной задачей и составлять алгоритм их выполнения;

– обосновывать и осуществлять выбор наиболее эффективных способов решения учебных и познавательных задач;

– определять/находить, в том числе из предложенных вариантов, условия для выполнения учебной и познавательной задачи;

– выстраивать жизненные планы на краткосрочное будущее (заявлять целевые ориентиры, ставить адекватные им задачи и предлагать действия, указывая и обосновывая логическую последовательность шагов);

– выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;

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

– определять потенциальные затруднения при решении учебной и познавательной задачи и находить средства для их устранения;

– описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;

– определять совместно с педагогом и сверстниками критерии планируемых результатов и критерии оценки своей учебной деятельности;

– систематизировать (в том числе выбирать приоритетные) критерии планируемых результатов и оценки своей деятельности;

– отбирать инструменты для оценивания своей деятельности, осуществлять самоконтроль своей деятельности в рамках предложенных условий и требований;

– 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;

– устанавливать связь между полученными характеристиками продукта и характеристиками процесса деятельности и по завершении деятельности предлагать изменение характеристик процесса для получения улучшенных характеристик продукта;

– сверять свои действия с целью и, при необходимости, исправлять ошибки самостоятельно;

– определять критерии правильности (корректности) выполнения учебной задачи;

– анализировать и обосновывать применение соответствующего инструментария для выполнения учебной задачи;

– свободно пользоваться выработанными критериями оценки и самооценки, исходя из цели и имеющихся средств, различая результат и способы действий;

– оценивать продукт своей деятельности по заданным и/или самостоятельно определенным критериям в соответствии с целью деятельности;

– обосновывать достижимость цели выбранным способом на основе оценки своих внутренних ресурсов и доступных внешних ресурсов;

– фиксировать и анализировать динамику собственных образовательных результатов.

– наблюдать и анализировать собственную учебную и познавательную деятельность и деятельность других обучающихся в процессе взаимопроверки;

– соотносить реальные и планируемые результаты индивидуальной образовательной деятельности и делать выводы;

– принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия

В результате освоения учебного курса обучающийся сможет:

– выделять общий признак двух или нескольких предметов или явлений, объяснять их сходство;

– объединять предметы и явления в группы по определенным признакам, сравнивать, классифицировать и обобщать факты и явления;

– 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;

– строить рассуждение на основе сравнения предметов и явлений, выделяя при этом общие признаки;

– излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;

– самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;

– вербализовать эмоциональное впечатление, оказанное на него источником;

– объяснять явления, процессы, связи и отношения, выявляемые в ходе познавательной и исследовательской деятельности (приводить объяснение с изменением формы представления; объяснять, детализируя или обобщая; объяснять с заданной точки зрения);

– делать вывод на основе критического анализа разных точек зрения, подтверждать вывод собственной аргументацией или самостоятельно полученными данными;

– переводить сложную по составу (многоаспектную) информацию из графического или формализованного (символьного) представления в текстовое, и наоборот;

– анализировать/рефлексировать опыт разработки и реализации учебного проекта, исследования (теоретического, эмпирического) на основе предложенной проблемной ситуации, поставленной цели и/или заданных критериев оценки продукта/результата.

– критически оценивать содержание и форму текста;

– определять необходимые ключевые поисковые слова и запросы;

– осуществлять взаимодействие с электронными поисковыми системами, словарями;

– формировать множественную выборку из поисковых источников для объективизации результатов поиска;

– соотносить полученные результаты поиска со своей деятельностью.

Коммуникативные универсальные учебные действия

В результате освоения учебного курса обучающийся сможет:

– определять возможные роли в совместной деятельности;

– играть определенную роль в совместной деятельности;

– принимать позицию собеседника, понимая позицию другого, различать в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории;

– определять свои действия и действия партнера, которые способствовали или препятствовали продуктивной коммуникации;

– строить позитивные отношения в процессе учебной и познавательной деятельности;

– корректно и аргументированно отстаивать свою точку зрения, в дискуссии уметь выдвигать контраргументы, перефразировать свою мысль (владение механизмом эквивалентных замен);

– критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;

– предлагать альтернативное решение в конфликтной ситуации;

– выделять общую точку зрения в дискуссии;

– договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;

– организовывать учебное взаимодействие в группе (определять общие цели, распределять роли, договариваться друг с другом и т. д.);

– устранять в рамках диалога разрывы в коммуникации,

– обусловленные непониманием/неприятием со стороны собеседника задачи, формы или содержания диалога;

– определять задачу коммуникации и в соответствии с ней отбирать речевые средства;

– отбирать и использовать речевые средства в процессе коммуникации с другими людьми (диалог в паре, в малой группе и т. д.);

– представлять в устной или письменной форме развернутый план собственной деятельности;

– соблюдать нормы публичной речи, регламент в монологе и дискуссии в соответствии с коммуникативной задачей;

– высказывать и обосновывать мнение (суждение) и запрашивать мнение партнера в рамках диалога;

– принимать решение в ходе диалога и согласовывать его с собеседником;

– создавать письменные «клишированные» и оригинальные тексты с использованием необходимых речевых средств;

– использовать вербальные средства (средства логической связи) для выделения смысловых блоков своего выступления;

– использовать невербальные средства или наглядные материалы, подготовленные/отобранные под руководством учителя;

– 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 результаты

Обучающийся научится:

– целеполаганию, включая постановку новых целей, преобразование практической задачи в познавательную;

– самостоятельно анализировать условия достижения цели на основе учета выделенных учителем ориентиров действия в новом учебном материале;

– уметь самостоятельно контролировать свое время и управлять им.

– учитывать разные мнения и стремиться к координации различных позиций в сотрудничестве;

– задавать вопросы, необходимые для организации собственной деятельности и сотрудничества с партнером;

– осуществлять взаимный контроль и оказывать в сотрудничестве необходимую взаимопомощь.

– давать определение понятиям;

– устанавливать причинно-следственные связи;

– осуществлять логическую операцию установления родовидовых отношений, ограничение понятия;

– обобщать понятия — осуществлять логическую операцию перехода от видовых признаков к родовому понятию, от понятия с меньшим объемом к понятию с большим объемом;

– строить логическое рассуждение, включающее установление причинно-следственных связей.

– осуществлять информационное подключение к локальной сети и глобальной сети Интернет;

– входить в информационную среду ОО, в том числе через Интернет, размещать в информационной среде различные информационные объекты;

– выводить информацию на бумагу, правильно обращаться с расходными материалами;

– соблюдать требования техники безопасности, гигиены, эргономики и ресурсосбережения при работе с устройствами ИКТ, в частности учитывающие специфику работы с различными экранами.

– находить в тексте требуемую информацию (пробегать текст глазами, определять его основные элементы, сопоставлять формы выражения информации в запросе и в самом тексте, устанавливать, являются ли они тождественными или синонимическими, находить необходимую единицу информации в тексте).

II. Содержание тем учебного предмета

Безопасность общения

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети. Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах. Персональные данные. Публикация личной информации. Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. Настройки приватности публичных страниц. Правила ведения публичных страниц. Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Формы деятельности: Аудиторное занятие.

Виды деятельности: Учащиеся беседуют с учителем. Обучающиеся записывают определения в тетради или выполняют практические задания с помощью компьютера.

Безопасность устройств

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов. 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. Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов. Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Формы деятельности: Аудиторное занятие.

Виды деятельности: Учащиеся беседуют с учителем. Обучающиеся записывают определения в тетради или выполняют практические задания с помощью компьютера.

Безопасность информации

Приемы социальной инженерии. Правила безопасности при виртуальных контактах. Фейковые новости. Поддельные страницы. Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов. Уязвимости Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях. Безопасность личной информации. Создание резервных копий на различных устройствах.

Формы деятельности: Аудиторное занятие.

Виды деятельности: Учащиеся беседуют с учителем. Обучающиеся записывают определения в тетради или выполняют практические задания с помощью компьютера.

III. Тематическое планирование

8 класс (34 часов)

№ занятия	Название раздела, темы	Кол-во часов
1	Что такое вредоносный код	5
2	Распространение вредоносного кода	5
3	Методы защиты от вредоносных программ	5
4	Распространение вредоносного кода для мобильных устройств	5
5	Подготовка к итоговому тесту	1
6	Выполнение теста	1
7	Работа над ошибками	1
8	Обсуждение тем индивидуальных и групповых проектов	2
9	Выполнение и защита индивидуальных и групповых проектов	5
10	Повторение	4
	Итого	**34**

9 класс (34 часов)

№ занятия	Название раздела, темы	Кол-во часов
1	Социальная инженерия: распознать и избежать	4
2	Ложная информация в Интернете	6
3	Безопасность при использовании платежных карт в Интернете	4
4	Беспроводная технология связи	4
5	Резервное копирование данных	4
6	Подготовка к итоговому тесту	1
7	Выполнение теста	1
8	Обсуждение тем индивидуальных и групповых проектов	2
9	Выполнение и защита индивидуальных и групповых проектов	5
10	Повторение	3
	Итого	**34**

Календарно-тематическое планирование 8 класс

№	Тема	Кол.-во часов	Дата		
			8а	8б	8в
1.	Что такое вредоносный код	1			
2.	Виды вредоносных кодов.	1			
3.	Возможности вредоносных кодов.	1			
4.	Деструктивные функции вредоносных кодов.	1			
5.	Распространение вредоносного кода.	1			
6.	Способы доставки вредоносных кодов.	1			
7.	Исполняемые файлы	1			
8.	Расширения вредоносных кодов.	1			
9.	Вредоносная рассылка.	1			
10.	Вредоносные скрипты.	1			
11.	Способы выявления наличия вредоносных кодов на устройствах.	1			
12.	Действия при обнаружении вредоносных кодов на устройствах.	1			
13.	Методы защиты от вредоносных программ	1			
14.	Способы защиты устройств от вредоносного кода	1			
15.	Антивирус или брандмауэр?	1			
16.	Антивирусные программы и их характеристики.	1			
17.	Выбор оптимального антивирусного ПО для ПК	1			
18.	Правила защиты от вредоносных кодов.	1			
19.	Распространение вредоносного кода для мобильных устройств	1			
20.	Расширение вредоносных кодов для мобильных устройств.	1			
21.	Правила безопасности при установке приложений на мобильные устройства	1			
22.	Современные системы идентификации устройств.	1			
23.	Подготовка к итоговому тесту	1			
24.	Выполнение теста	1			
25.	Работа над ошибками	1			
26.	Проектная деятельность. Этапы выполнения проекта.	1			
27.	Обсуждение тем индивидуальных и групповых проектов	1			
28.	Выбор темы проекта, цели, задачи	1			
29.	Выполнение индивидуальных и групповых проектов	1			
30.	Выполнение индивидуальных и групповых проектов	1			
31.	Выполнение индивидуальных и групповых проектов	1			
32.	Защита проектов	1			
33.	Повторение	1			
34.	Повторение	1			

Календарно-тематическое планирование 9 класс

№	Тема	Кол.-во часов	Дата		
			9а	9б	9в
35.	Социальная инженерия: распознать и избежать	1			
36.	Приемы социальной инженерии.	1			
37.	Правила безопасности при виртуальных контактах.	1			
38.	Ложная информация в Интернете	1			
39.	Фейковые новости.	1			
40.	Поддельные страницы.	1			
41.	Как распознать поддельную страницу	1			
42.	Проверка новостей на фейк	1			
43.	Безопасность при использовании платежных карт в Интернете	1			
44.	Транзакции и связанные с ними риски.	1			
45.	Правила совершения онлайн-покупок.	1			
46.	Безопасность банковских сервисов.	1			
47.	Беспроводная технология связи	1			
48.	Уязвимости Wi-Fi-соединений.	1			
49.	Публичные и непубличные сети.	1			
50.	Правила работы в публичных сетях.	1			
51.	Резервное копирование данных	1			
52.	Безопасность личной информации.	1			
53.	Создание резервных копий на различных устройствах.	1			
54.	Создание резервных копий на ПК	1			
55.	Создание резервных копий на мобильных устройствах	1			
56.	Подготовка к итоговому тесту	1			
57.	Выполнение теста	1			
58.	Работа над ошибками	1			
59.	Что такое проектная деятельность.	1			
60.	Обсуждение тем индивидуальных и групповых проектов	1			
61.	Выбор темы проекта, цели, задачи	1			
62.	Выполнение индивидуальных и групповых проектов	1			
63.	Выполнение индивидуальных и групповых проектов	1			
64.	Выполнение индивидуальных и групповых проектов	1			
65.	Защита проектов	1			
66.	Защита проектов				
67.	Повторение	1			
68.	Повторение	1			

8 класс

ОСНОВНЫЕ КРИТЕРИИ ОЦЕНИВАНИЯ ДЕЯТЕЛЬНОСТИ ОБУЧАЮЩИХСЯ

Тест по теме «Безопасность устройств»

1. Какие программы (коды) можно назвать вредоносными?
   1) Программы, ворующие регистрационные данные.
   2) Программы, использующие ресурсы других компьютеров.
   3) Программы, дающие несанкционированный доступ к ключевым файлам различных программных продуктов.
   4) Программы, использующие ресурсы компьютеров в интересах своего автора.
   5) Программы, предлагающие посетить платные веб-ресурсы.
   6) Программы, принудительно демонстрирующие рекламную информацию.
   7) Программы, проникающие в системные области данных и меняющие их.
   8) Программы, исправляющие ошибки и недоработки в новых версиях приложений.
   9) Программы, шифрующие персональные файлы пользователя.
2. Составьте список вредоносных программ, созданных злоумышленниками для того, чтобы:
   1) Получить доступ к электронным финансам пользователя.
   2) Зашифровать пользовательские данные и выманить деньги у пользователя за расшифровку.
   3) Организовать сетевую атаку на сервер организации с целью дальнейшего шантажа.
   4) Создать сеть централизованно управляемых компьютеров для продажи управления ими.
   5) Проникнуть в клиентские базы данных, финансовую и техническую документацию компаний с целью получения ценной информации.
3. Проанализируйте и отметьте истинные (верные) высказывания.
   1) Трояны распространяются самостоятельно, а вирусы распространяют люди.
   2) Трояны распространяют люди, а вирусы распространяются самостоятельно.
   3) Трояны, распространяются так же, как и вирусы.
   4) Черви распространяются так же, как и вирусы.
   5) Черви распространяют люди.
4. Как распространяются вредоносные программы?
   1) С помощью вложенных в письма файлов.
   2) При скачивании приложений.
   3) При авторизации в социальных сетях.
   4) При посещении популярных сайтов.
   5) С помощью файлообменных сетей и торрентов.
   6) С помощью методов социальной инженерии.
   7) При переходе по ссылке для подтверждения регистрации.
   8) При использовании заражённой интернет-страницы.
   9) Компаниями, которые создают и продают защиту от вредоносных программ.
   10) Предлагаются телефонным провайдером.
5. Выделите действия, которые связаны с целью установления обновлений и являются обязательными для защиты от проникновения вредоносных программ.
   1) Обновлять операционную систему для устранения в новых версиях ошибок и уязвимостей.
   2) Не обновлять операционную систему, потому что обновления тоже могут содержать ошибки, которые представляют опасность.
   3) Не обновлять лицензионную операционную систему, потому что она достаточно безопасная.

4) Обновлять браузер, потому что в новых версиях исправляют уязвимости и недостатки предыдущих версий.

5) Не обновлять браузер, игнорировать информацию о необходимости обновления, потому что она бессмысленна.

6) Не обновлять браузер, потому что при обновлении могут быть занесены вредоносные программы.

7) Обновлять антивирусное программное обеспечение для детектирования и блокирования вновь появившихся вредоносных программ.

8) Не обновлять антивирусное программное обеспечение, потому что оно лишь добавит новые функции или изменит интерфейс и будет платным.

9) Не обновлять антивирусное программное обеспечение до истечения платной лицензии.

6. При работе с поисковыми браузерами вы находите известный вам сайт, но появляется предупреждение об опасности. Выберите ваши действия.

1) Не буду заходить на сайт, даже проверенный сайт может быть заражён.

2) Не буду обращать внимание на предупреждение, потому что уже заходил на этот сайт неоднократно, и перейду на сайт.

3) Поищу информацию о заражении этого сайта, и если не найду, то перейду на сайт.

7. Выберите самое точное определение человека, не застрахованного от проникновения разного рода вредоносных программ на устройства, которыми он пользуется.

1) Внимательный и аккуратный человек.

2) Невнимательный и неаккуратный человек.

3) Человек, следящий за обновлениями браузера, операционной системы и антивирусного программного обеспечения.

4) Человек, не следящий за обновлениями браузера, операционной системы и антивирусного программного обеспечения.

5) Не разбирающийся в устройствах и программах человек.

6) Разбирающийся в устройствах и программах человек.

7) Любой человек.

8. Какие программы называются эксплойтами?

1) Вредоносные программы, которые маскируются под полезные утилиты.

2) Компьютерные программы, использующие уязвимости в программном обеспечении.

3) Вредоносные программы, которые скрытно действуют и затрудняют их обнаружение системами безопасности.

9. На какие параметры антивирусных программ следует обращать внимание при покупке?

1) Разнообразие функций.

2) Уровень детектирования.

3) Бесплатность.

4) Платность.

5) Влияние на скорость работы компьютера.

6) Уровень ложных срабатываний.

7) Доставка обновлений.

8) Наличие лицензии.

9) Продление лицензии.

10. Напишите пять и более правил, которые необходимо соблюдать продвинутому пользователю для осуществления защиты от вредоносных программ.

11. Отметьте виды программ, которые всегда вредоносны.

1) Вирусы.

2) Черви.

3) Трояны.

4) Скрипты.

5) Макросы.

6) Архиваторы.
7) Бэкдоры.
8) Буткиты.
9) Утилиты.

12. Отметьте, что необходимо использовать на компьютере, чтобы предотвратить заражение вирусами.

1) Регулярное обновление браузера.
2) Регулярное обновление операционной системы.
3) Регулярное обновление антивирусной базы.
4) Проверку адресов сайтов.
5) Отказ от перехода по ссылкам из всплывающих окон.
6) Использование диспетчера задач для закрытия браузера в случае заражения.
7) Загрузку программного обеспечения только с официальных сайтов-разработчиков.
8) Выбор зарекомендовавших себя антивирусных программ.
9) Установку только лицензионных версий программного обеспечения.
10) Установку проактивного и поведенческого анализа в антивирусной базе.
11) Проверку почтовых сообщений и их вложений.
12) Полное сканирование компьютера и подключаемых устройств не реже одного раза в неделю.
13) Установку на компьютер сразу нескольких средств защиты.

Темы проектов:

1. Спрос рождает предложение или предложение рождает спрос на рынке антивирусного программного обеспечения.
2. Нормативно-правовая база в законодательстве РФ по вопросам охраны баз данных, защиты личной информации и электронной подписи, авторского права на программу или приложение, права распространения информации и использования персональных данных в Интернете.
3. Полезные навыки для обеспечения безопасности устройств.
4. Какой ущерб наносит обществу компьютерное пиратство?
5. Современные системы идентификации устройств.
6. Основные компоненты компьютерной грамотности, которые необходимы человеку для безопасной жизни в современном цифровом обществе.

Ключи ответов к тесту по теме «Безопасность устройств»

Номер задания	**Правильный ответ**
1	ворующие регистрационные данные; дающие несанкционированный доступ к ключевым файлам различных программных продуктов; использующие ресурсы компьютеров в интересах своего автора; программы, проникающие в системные области данных и меняющие их; программы, шифрующие персональные файлы пользователя
2	Возможные ответы: трояны-клавиатурные шпионы; трояны-шифровальщики; программы, организующие зомби-сети, и атаку с них; специализированные программы-боты; сетевые черви. Ответами могут быть конкретные названия троянов, червей, приложений и ботнетов
3	Трояны распространяют люди, а вирусы распространяются самостоятельно. Черви распространяются так же, как и вирусы.

4	с помощью вложенных в письма файлов при скачивании приложений при посещении популярных сайтов с помощью файлообменных сетей и торрентов с помощью методов социальной инженерии при использовании заражённой интернет-страницы компаниями, которые создают и продают защиту от вредоносных программ
5	обновлять операционную систему для устранения в новых версиях ошибок и уязвимости; обновлять браузер, потому что в новых версиях исправляют уязвимости и недостатки предыдущих версий; обновлять антивирусное программное обеспечение, для детектирования и блокирования вновь появившихся вредоносных программ
6	Не буду заходить на сайт, даже проверенный сайт может быть заражён
7	Любой человек
8	компьютерные программы, использующие уязвимости в программном обеспечении
9	разнообразие функций уровень детектирования доставка обновлений наличие лицензии продление лицензии
10	Возможные ответы: Использовать антивирусное ПО. Своевременно обновлять ПО, операционную систему, браузер и приложения. Проверять приходящие файлы и ссылки перед скачиванием и открытием. Проявлять интерес к информации от антивирусных компаний и экспертов по компьютерной безопасности. Не проводить процедуру получения прав суперпользователя на устройствах. Не скачивать файлы с подозрительных источников. Обращать внимание на расширение загружаемого файла. Воздержаться от загрузки пиратской версии программ, а скачивать файлы с официального сайта производителя. Не скачивать приложение в комплекте с дополнительным ПО. Читать отзывы и советоваться с родителями и друзьями
11	Вирусы Черви Трояны Бэкдоры Руткиты
12	регулярное обновление браузера регулярное обновление операционной системы регулярное обновление антивирусной базы проверка адресов сайтов отказ от перехода по ссылкам из всплывающих окон использование диспетчера задач для закрытия браузера в случае заражения загрузка ПО только с официальных сайтов-разработчиков выбор зарекомендовавших себя антивирусных программ установка только лицензионных версий ПО установка проактивного и поведенческого анализа в антивирусной базе проверка почтовых сообщений и их вложений полное сканирование компьютера и подключаемых устройств не реже 1раза в неделю

Требования к содержанию итоговых проектно-исследовательских работ

Критерии содержания текста проектно-исследовательской работы

1. Во введении сформулирована актуальность (личностную и социальную значимость) выбранной проблемы. Тема может быть переформулирована, но при этом чётко определена, в необходимости исследования есть аргументы.
2. Правильно составлен научный аппарат работы: точность формулировки проблемы, чёткость и конкретность в постановке цели и задач, определении объекта и предмета исследования, выдвижении гипотезы. Гипотеза сформулирована корректно и соответствуют теме работы.
3. Есть планирование проектно-исследовательской деятельности, корректировка её в зависимости от результатов, получаемых на разных этапах развития проекта. Дана характеристика каждого этапа реализации проекта, сформулированы задачи, которые решаются на каждом этапе, в случае коллективного проекта — распределены и выполнены задачи каждым участником, анализ ресурсного обеспечения проекта проведён корректно.
4. Используется и осмысляется междисциплинарный подход к исследованию и проектированию и на базовом уровне школьной программы, и на уровне освоения дополнительных библиографических источников.
5. Определён объём собственных данных и сопоставлено собственное проектное решение с аналоговыми по проблеме. Дан анализ источников и аналогов с точки зрения значимости для собственной проектно-исследовательской работы, выявлена его новизна, библиография и интернет-ресурсы грамотно оформлены.
6. Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения.
7. Есть оценка результативности проекта, соотнесение с поставленными задачами. Проведена оценка социокультурных и образовательных последствий проекта на индивидуальном и общественном уровнях.

Критерии презентации проектно-исследовательской работы (устного выступления)

1. Демонстрация коммуникативных навыков при защите работы. Владение риторическими умениями, раскрытие автором содержания работы, достаточная осведомлённость в терминологической системе проблемы, отсутствие стилистических и речевых ошибок, соблюдение регламента.
2. Умение чётко отвечать на вопросы после презентации работы.
3. Умение создать качественную презентацию. Демонстрация умения использовать IT-технологии и создавать слайд презентацию на соответствующем его возрасту уровне.
4. Умение оформлять качественный презентационный буклет на соответствую-ем его возрасту уровне.
5. Творческий подход к созданию продукта, оригинальность, наглядность, иллюстративность. Предоставлен качественный творческий продукт (макет, программный продукт, стенд, статья, наглядное пособие, литературное произведение, видео-ролик, мультфильм и т. д.).
6. Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность намечать пути сотрудничества на уровне взаимодействия с членами кружка или секции, проявление в ходе презентации коммуникабельности, благодарности и уважения по отношению к руководителю, консультантам, умение чётко обозначить пути создания сетевого продукта.
7. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути её исследования и проектного решения.

9 класс

ОСНОВНЫЕ КРИТЕРИИ ОЦЕНИВАНИЯ ДЕЯТЕЛЬНОСТИ ОБУЧАЮЩИХСЯ

Тест по теме «Безопасность информации»

1. Подберите синонимичные прилагательные на русском языке и объясните следующие понятия:
   1) Фейковые новости.
   2) Фейковая программа.
   3) Фейковый номер телефона.
   4) Фейковый аккаунт.
   5) Фейковая страница в социальной сети.
   6) Фейковая кредитная карта.
   7) Фейковый профиль.
   8) Фейковый сайт.

Возможные ответы:

А) Фальшивые новости, ложно смонтированные видео.

Б) Приложение, которое имеет дизайн и функционал, напоминающий переделываемую программу.

В) Виртуальный номер телефона.

Г) Любой аккаунт с недостоверной информацией — имя, контакты, фотографии.

Д) Фиктивная страница в интернет-ресурсах.

Е) Банковская карта, оформленная на человека, который в реальности не существует.

Ж) Профиль, содержащий ложную информацию о владельце либо не содержащий её вовсе.

З) Фальсифицированный сайт, копия главной страницы которого напоминает известный.

2. С какими областями деятельности людей чаще всего связаны фейки?
   1) Политика.
   2) Наука.
   3) Реклама и продвижение товаров.
   4) Торговля.
   5) Обучение.
   6) Производство.
   7) Маркетинг.
   8) Изобретения.
   9) Артистическая сфера.
   10) Путешествия.

3. Сколько источников и какие именно необходимо просмотреть, чтобы сравнить факты и сделать вывод: является ли эта новость фейковой? Укажите свои источники или выберите из предложенных.

Выберите количество: 1, 2, 3, 4, 5.

Выберите из предложенных источников:
   1) Официальное СМИ.
   2) Неофициальное СМИ.
   3) Википедия.
   4) Интернет-источник.

4. Выберите правильный ответ. Социальная инженерия — это:

1) Привлечение пользователя к действиям, способствующим заражению вредоносными программами.

2) Метод управления действиями человека без использования технических средств.

3) Технология внедрения вредоносных программ, использующая управление действиями пользователя.

5. Отметьте места, в которых можно безопасно подключиться к общественной сети Wi-Fi.

1) Кафе.
2) Школа.
3) Общественный транспорт.
4) Такси.
5) Ресторан.
6) Торговый центр.
7) Поликлиника.
8) Вуз.

6. Какое шифрование сети, предназначенное для её защиты, легко взломать?
1) WPA.
2) WPA2.
3) WEP.

7. Каковы дополнительные признаки безопасности публичной Wi-Fi-сети?
1) Рядом со значком Wi-Fi находится замочек.
2) Для входа в сеть требуется авторизация.
3) Для входа в сеть необходимо ввести пароль.
4) Название сети совпадает с названием учреждения или места расположения.

8. Какие меры безопасности необходимы для проведения онлайн-платежей?
1) Операционная система обновлена.
2) Версия браузера обновлена.
3) Двухфакторная онлайн-транзакция.
4) Компьютер друзей.
5) Свой компьютер.
6) Антивирус, установленный на устройстве, с которого производится транзакция.
7) Обновлённый антивирус, установленный на устройстве, с которого производится транзакция.
8) Правильный адрес в адресной строке.
9) Банковское приложение, скачанное с официального сайта банка.
10) Банковское приложение, скачанное из магазина приложений.
11) Ссылка на страницу из электронного письма или другого источника на онлайн-банкинг.

9. Распределите у себя в тетрадях предложенные действия по столбцам в соответствии с целями необходимости резервного копирования данных.
1) Хранение первоначальной версии операционной системы, не заражённой вредоносными программами.
2) Возможность использования и сохранения последней версии реферата, доклада или других рабочих документов.
3) Защита информации от вредоносного программного обеспечения.
4) Защита от физической порчи флеш-карты.
5) Защита от физической порчи жёсткого диска.
6) Хранение ценных файлов и данных на любом устройстве.

От сбоев оборудования	От случайной потери или искажения хранящейся информации	От несанкционированного доступа к информации

10. Напишите 5 симптомов вероятного заражения вашего устройства вредоносными программами.

Темы проектов:

1. Фейки — это хорошо или плохо?
2. Как проводить маркетинговые исследования онлайн?
3. Достоинства и недостатки онлайн-шопинга.
4. Криптография для защиты информации.
5. Социальные информационные технологии: позитивные, негативные и нейтральные.
6. Манипулирование общественным сознанием в социальных сетях.
7. Особенности рекламы онлайн.

Ключи ответов к тесту по теме **«Безопасность информации»**

<table>
<tr><th>Номер задания</th><th>Правильный ответ</th></tr>
<tr><td>1</td><td>Возможные ответы: А) фальшивые новости, ложно смонтированные видео; Б) приложение, которые имеет дизайн и функционал, напоминающий переделываемую программу; В) виртуальный номер телефона; Г) любой аккаунт с недостоверной информацией — имя, контакты, фотографии; Д) фиктивная страница в интернет-ресурсах; Е) банковская карта, оформленная на человека, который в реальности не существует; Ж) профиль, содержащий ложную информацию о владельце либо не содержащую вовсе; З) сайт фальсифицированный, копия главной страницы которого напоминает известный</td></tr>
<tr><td>2</td><td>Политика
Реклама и продвижение товаров
Торговля
Маркетинг
Артистическая сфера</td></tr>
<tr><td>3</td><td>3, 4, 5
Возможный ответ: Википедия в сочетании в другими источниками, но не менее трёх разных источников</td></tr>
<tr><td>4</td><td>технология внедрения вредоносных программ, использующая управление действиями пользователя</td></tr>
<tr><td>5</td><td>школа;
общественный транспорт;
поликлиника;
ВУЗ</td></tr>
<tr><td>6</td><td>WEP</td></tr>
<tr><td>7</td><td>замочек рядом со значком Wi-Fi
Авторизация в Сети
Wi-Fi с паролем доступа</td></tr>
<tr><td>8</td><td>операционная система обновлена
версия браузера обновлена
двухфакторная онлайн-транзакция
свой компьютер
обновлённый антивирус, установленный на устройстве, с которого производится транзакция
правильный адрес в адресной строке
банковское приложение, скачанное с официального сайта банка</td></tr>
<tr><td>9</td><td>Правильное распределение:
<table>
<tr><td>От сбоев оборудования</td><td>От случайной потери или искажения хранящейся информации</td><td>От несанкционированного доступа к информации</td></tr>
<tr><td>защита от физической</td><td>возможность</td><td>защита информации от</td></tr>
</table>
</td></tr>
</table>

	порчи жёсткого диска защита от физической порчи флеш-карты	использования и сохранения последней версии реферата, доклада или других рабочих документов хранение ценных файлов и данных на любом устройстве	вредоносного ПО хранение первоначальной версии операционной системы, не заражённой вредоносными программами
10	Возможные ответы: некоторые программы перестают работать, на экран выводятся посторонние сообщения или символы, работа существенно замедляется, некоторые файлы не открываются или оказываются испорченными, операция сохранения файлов или какая-нибудь другая операция происходит без команды пользователя		

Требования к содержанию итоговых проектно-исследовательских работ

Критерии содержания текста проектно-исследовательской работы

1. Во введении сформулирована актуальность (личностную и социальную значимость) выбранной проблемы. Тема может быть переформулирована, но при этом чётко определена, в необходимости исследования есть аргументы.
2. Правильно составлен научный аппарат работы: точность формулировки проблемы, чёткость и конкретность в постановке цели и задач, определении объекта и предмета исследования, выдвижении гипотезы. Гипотеза сформулирована корректно и соответствуют теме работы.
3. Есть планирование проектно-исследовательской деятельности, корректировка её в зависимости от результатов, получаемых на разных этапах развития проекта. Дана характеристика каждого этапа реализации проекта, сформулированы задачи, которые решаются на каждом этапе, в случае коллективного проекта — распределены и выполнены задачи каждым участником, анализ ресурсного обеспечения проекта проведён корректно.
4. Используется и осмысляется междисциплинарный подход к исследованию и проектированию и на базовом уровне школьной программы, и на уровне освоения дополнительных библиографических источников.
5. Определён объём собственных данных и сопоставлено собственное проектное решение с аналоговыми по проблеме. Дан анализ источников и аналогов с точки зрения значимости для собственной проектно-исследовательской работы, выявлена его новизна, библиография и интернет-ресурсы грамотно оформлены.
6. Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения.
7. Есть оценка результативности проекта, соотнесение с поставленными задачами. Проведена оценка социокультурных и образовательных последствий проекта на индивидуальном и общественном уровнях.

Критерии презентации проектно-исследовательской работы (устного выступления)

1. Демонстрация коммуникативных навыков при защите работы. Владение риторическими умениями, раскрытие автором содержания работы, достаточная осведомлённость в терминологической системе проблемы, отсутствие стилистических и речевых ошибок, соблюдение регламента.
2. Умение чётко отвечать на вопросы после презентации работы.
3. Умение создать качественную презентацию. Демонстрация умения использовать IT-технологии и создавать слайд презентацию на соответствующем его возрасту уровне.
4. Умение оформлять качественный презентационный буклет на соответствую-ем его возрасту уровне.

5. Творческий подход к созданию продукта, оригинальность, наглядность, иллюстративность. Предоставлен качественный творческий продукт (макет, программный продукт, стенд, статья, наглядное пособие, литературное произведение, видео-ролик, мультфильм и т. д.).
6. Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность намечать пути сотрудничества на уровне взаимодействия с членами кружка или секции, проявление в ходе презентации коммуникабельности, благодарности и уважения по отношению к руководителю, консультантам, умение чётко обозначить пути создания сетевого продукта.
7. Ярко выраженный интерес к научному поиску, самостоятельность в выборе
проблемы, пути её исследования и проектного решен

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 141801485388770673109170416287983275056075262737

Владелец Абуляев Рафик Рашитович

Действителен С 09.10.2023 по 08.10.2024