МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования и науки Республики Татарстан
Исполнительный комитет Спасского муниципального района
Республики Татарстан
МБОУ "Никольская СОШ"

«СОГЛАСОВАНО»	«УТВЕРЖДЕНО»
на заседании	Директор школы
педагогического совета	О.Ю.Федорова
Протокол №1	Приказ №70
от «26» августа 2025 г.	от «27» августа 2025 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 00DF3E4832C387435BAB1766AC10640423
Владелец Федорова Ольга Юрьевна
Действителен с 24.03.2025 до 17.06.2026

РАБОЧАЯ ПРОГРАММА

учебного курса «Компьютерная и информационная безопасность»

для обучающихся 8 класса

с.Никольское 2025 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа учебного курса «Компьютерная и информационная безопасность» составлена для учащихся 8 класса Муниципального бюджетного общеобразовательного учреждения «Никольская СОШ» Спасского муниципального района Республики Татарстан, направлена на достижение следующих планируемых результатов Федерального государственного образовательного стандарта основного общего образования:

- предметных;
- метапредметных (регулятивных, познавательных, коммуникативных);
- личностных.

Курс является важной составляющей частью работы с учащимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.), задумывающимися о своей личной безопасности, безопасности своей семьи и своих друзей, а также проявляющими интерес к изучению истории и технологических основ информационной безопасности.

Программа курса ориентирована на выполнение требований Федерального государственного образовательного стандарта основного общего образования к организации и содержанию внеурочной деятельности школьников. Ее реализация даёт возможность раскрытия индивидуальных способностей школьников, развития интереса к различным видам индивидуальной и групповой деятельности, закрепления умения самостоятельно организовать свою учебную, в том числе проектную деятельность.

Цель программы:

- формирование активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им;
- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз.

Задачи программы:

- дать представление о современном информационном обществе, информационной безопасности личности и государства;
- сформировать навыки ответственного и безопасного поведения современной информационно-телекоммуникационной среде;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом;
- сформировать общекультурные навыки работы с информацией (умений грамотно пользоваться источниками информации, правильно организовать информационный процесс);
- дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;
- познакомить со способами защиты от противоправных посягательств в сети Интернет, защиты личных данных.

Содержание программы соответствует темам примерной основной образовательной программы основного общего образования (ПООП ООО) учебного предмета «Информатика», а также расширяет их за счёт привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных

компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребёнка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание модуля Программы представлено разделами «Безопасность общения», «Безопасность устройств»», «Безопасность информации». Система учебных заданий, предложенная в модуле, позволяет создать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень её опасности, предвидеть последствия информационной угрозы и противостоять им, и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищённости детей от информационных рисков и угроз. Система заданий предполагает индивидуальную и групповую формы работы, составление памяток, анализ защищённости собственных аккаунтов в социальных сетях и электронных сервисах, практические работы. Предлагаемые задания направлены на формирование критичного мышления школьников, формирование умений решать проблемы, работать в команде, высказывать и защищать собственную позицию, приобретение основ безопасной работы с информацией в виртуальном мире.

Каждый раздел программы завершается выполнением проверочного теста и проектной работой по одной из тем, предложенных на выбор учащимся. Эти занятия в качестве итоговой работы могут быть проведены учащимися, освоившими программу. Для проведения таких занятий могут быть использованы презентации, проекты, памятки и т.д. , подготовленные в ходе выполнения заданий.

Формат оценки учащихся: зачет/незачет

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА

Раздел 1. БЕЗОПАСНОСТЬ ОБЩЕНИЯ

Тема 1. Общение в социальных сетях и мессенджерах

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

Тема 2. С кем безопасно общаться в интернете

Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты

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

Тема 5. Настройки конфиденциальности в социальных сетях

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

Тема 6. Публикация информации в социальных сетях

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг

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

Тема 8. Публичные аккаунты

Настройки приватности публичных страниц. Правила ведения публичных страниц.

Тема 9. Фишинг

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

Тема 10. Выполнение и защита индивидуальных и групповых проектов

Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. Цели, задачи, SMART. Защита проекта.

Раздел 2. БЕЗОПАСНОСТЬ УСТРОЙСТВ

Тема 1. Что такое вредоносный код

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода

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

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

Тема 4. Распространение вредоносного кода для мобильных устройств

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

Тема 5. Выполнение и защита индивидуальных и групповых проектов

Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. Цели, задачи, SMART. Защита проекта.

Раздел 3. БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

Тема 1. Социальная инженерия: распознать и избежать

Приемы социальной инженерии. Правила безопасности в виртуальных контактах.

Тема 2. Ложная информация в Интернете

Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете

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

Тема 4. Беспроводная технология связи

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

Тема 5. Резервное копирование данных

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Выполнение и защита индивидуальных и групповых проектов

Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. Цели, задачи, SMART. Защита проекта.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОГО КУРСА

Предметные результаты:

Научатся:

- 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;

Получат возможность

Овладеть:

- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п;
- основами самоконтроля, соблюдения норм информационной этики и права;
- навыками самостоятельного принятия решения и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности в сети интернет;

Метапредметные результаты.

Межпредметные понятия.

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.

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.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Содержание	Количество часов	ЦОР
	Раздел 1. БЕЗОПАСНОСТЬ ОБЩЕНИЯ		1. «Азбука Безопасности» - http://azbez.com/safety/internet 2. Портал Российского Оргкомитета по проведению Года Безопасного Интернета - http://www.saferinternet.ru/ 3. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Сети. Интернет-угрозы и эффективное противодействие им - http://saferunet.ru/ Центр безопасного Интернета в России. 4. Фонд развития интернета Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности с безопасности Интернета - www.fid.ru 5. «Основы безопасности детей и молодежи в Интернете» — интерактивный курс по Интернет-безопасности - http://laste.arvutikaitse.ee/rus/html/etusivu.htm 6. «Безопасность детей в интернете». Информация для родителей: памятки, советы, рекомендации - http://www.internet-kontrol.ru/stati/bezopasnost-detey-v-internete.html 7. Образовательно выставочный проект "Дети в Интернете" - http://detionline.com/mts/about 8. Детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному использованию сети Интернет - http://interneshka.net/ -
1.	**Тема 1. Общение в социальных сетях и мессенджерах**	**1**	
2.	**Тема 2. С кем безопасно общаться в интернете**	**1**	
3.	**Тема 3. Методы защиты от вредоносных программ**	**1**	
4.	**Тема 4. Безопасный вход в аккаунты**	**1**	
5.	**Тема 5. Настройки конфиденциальности в социальных сетях**	**1**	
6.	**Тема 6. Публикация информации в социальных сетях**	**1**	
7.	**Тема 7. Кибербуллинг**	**1**	
8.	**Тема 8. Публичные аккаунты**	**1**	
9.	**Тема 9. Фишинг**	**2**	
10.	**Выполнение и защита индивидуальных и групповых проектов**	**3**	
11.	**Обобщение изученного материала. Тестирование**	**1**	
	Итого:	**14**	

			«Интернешка».

№ п/п	Содержание	Количество часов	ЦОР
	Раздел 2. БЕЗОПАСНОСТЬ ИНФОРМАЦИИ		1. «Азбука Безопасности» - http://azbez.com/safety/internet 2. Портал Российского Оргкомитета по проведению Года Безопасного Интернета - http://www.saferinternet.ru/ 3. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Сети. Интернет-угрозы и эффективное противодействие им - http://saferunet.ru/ Центр безопасного Интернета в России. 4. Фонд развития интернета Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности с безопасности Интернета - www.fid.ru 5. «Основы безопасности детей и молодежи в Интернете» — интерактивный курс по Интернет-безопасности - http://laste.arvutikaitse.ee/rus/html/etusivu.htm 6. «Безопасность детей в интернете». Информация для родителей: памятки, советы, рекомендации - http://www.internet-kontrol.ru/stati/bezopasnost-detey-v-internete.html 7. Образовательно выставочный проект "Дети в Интернете" - http://detionline.com/mts/about 8. Детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному использованию сети Интернет - http://interneshka.net/ - «Интернешка».
1.	**Тема 1. Что такое вредоносный код**	**1**	
2.	**Тема 2. Распространение вредоносного кода**	**1**	
3.	**Тема 3. Методы защиты от вредоносных программ**	**2**	
4.	**Тема 4. Распространение вредоносного кода для мобильных устройств**	**1**	
5.	**Выполнение и защита индивидуальных и групповых проектов**	**3**	
6	**Обобщение изученного материала. Тестирование**	**1**	
	Итого:	**9**	

№ п/п	Содержание	Количество часов	ЦОР
	Раздел 3. БЕЗОПАСНОСТЬ УСТРОЙСТВ		1. «Азбука Безопасности» - http://azbez.com/safety/internet 2. Портал Российского Оргкомитета по проведению Года Безопасного Интернета - http://www.saferinternet.ru/ 3. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Сети. Интернет-угрозы и эффективное противодействие им - http://saferunet.ru/ Центр безопасного Интернета в России. 4. Фонд развития интернета Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности с безопасности Интернета - www.fid.ru 5. «Основы безопасности детей и молодежи в Интернете» — интерактивный курс по Интернет-безопасности - http://laste.arvutikaitse.ee/rus/html/etusivu.htm 6. «Безопасность детей в интернете». Информация для родителей: памятки, советы, рекомендации - http://www.internet-kontrol.ru/stati/bezopasnost-detey-v-internete.html 7. Образовательно выставочный проект "Дети в Интернете" - http://detionline.com/mts/about 8. Детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному
1.	**Тема 1. Социальная инженерия: распознать и избежать**	**1**	
2.	**Тема 2. Ложная информация в Интернете**	**1**	
3.	**Тема 3. Безопасность при использовании платежных карт в Интернете**	**1**	
4.	**Тема 4. Беспроводная технология связи**	**1**	
5.	**Тема 5. Резервное копирование данных**	**1**	
6.	**Выполнение и защита индивидуальных и групповых проектов**	**3**	
7	**Обобщение изученного материала. Тестирование**	**1**	
8	**Повторение и обобщение курса. Резерв.**	**2**	
	Итого:	**11**	

			использованию сети Интернет - http://interneshka.net/ - «Интернешка».

Приложение 1

ОСНОВНЫЕ КРИТЕРИИ ОЦЕНИВАНИЯ ДЕЯТЕЛЬНОСТИ ОБУЧАЮЩИХСЯ ПО МОДУЛЮ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ПРЕДМЕТА «ИНФОРМАТИКА» НА СТУПЕНИ ОСНОВНОГО ОБЩЕГО ОБРАЗОВАНИЯ

Тест по теме «Безопасность общения»

1. Установите соответствие между названиями функций браузера и их описанием.

1) История посещения страниц. 2) Защита от фишинга и вредоносного программного обеспечения. 3) Автозаполнение. 4) Управление информацией о местоположении. 5) Сохранение паролей. 6) Управление всплывающими окнами.	А. Упрощает доступ к регулярно посещаемым сайтам за счёт автоматического ввода. Б. Автоматическая блокировка всплывающих окон, чтобы они не загромождали экран. В. Использование данных о вашем местонахождении для вывода ближайших к вам запрашиваемых мест. Г. Доступ к регулярно посещаемым сайтам за счёт автоматического заполнения учётных данных. Д. Запрос на подтверждение операции при загрузке файла. Е. Возврат на посещённую страницу или восстановление события.

2. Выберите правильный ответ. Социальная сеть — это:
   1) Онлайн-сервис, предоставленный провайдером.
   2) Веб-сайт.
   3) Программное обеспечение, позволяющее переписываться.
   4) Онлайн-сервис в Интернете для общения и связи.
3. Соотнесите названия мессенджеров и сетей с их назначением и содержанием.
   1) Общение с использованием псевдонимов.
   2) Графический контент.
   3) Обсуждение новостей.
   4) Видео, фотографии, комментарии.
   5) Посты.
   6) Персональная информация пользователей. Twitter, ВКонтакте, Instagram, WhatsApp, Telegram, Facebook (или напишите свои).
4. Что такое аккаунт социальной сети?
   1) Веб-страница в Интернете.
   2) Учётная запись пользователя в каком-либо сервисе.
   3) Логин и пароль для входа в социальную сеть.
5. Выберите информацию, которую безопасно размещать на своей странице в Интернете для незнакомых людей.
   1) Домашний адрес.
   2) Номер школы, в которой учитесь.
   3) Паспортные данные или фотографию паспорта.

4) Геолокация устройства, с которого осуществляется ввод.
5) Секцию, в которую ходите.
6) Любимые места в городе.
7) Фотографии родителей, находящихся на отдыхе.
8) Ваше хобби.
9) Любимые книги.

6. Какие настройки приватности в социальных сетях следует установить, чтобы обезопасить себя от мошенников?
1) Приватность аудиозаписей.
2) Приватность фотографий.
3) Приватность списка друзей.
4) Приватность подарков.
5) Приватность персональных данных.
6) Приватность местоположения.

7. Отметьте простые (слабые) пароли для использования в учётной записи.
1) 654321ToPas&.
2) ytrewq.
3) Asdf123#Mnb.
4) drowssap.
5) uiop.
6) Mypassword.
7) Ivan1968.

8. Что можно отнести к двухфакторной аутентификации?
1) Логин и пароль от учётной записи на странице авторизации.
2) Логин и пароль от учётной записи и пароль из СМС-сообщения.
3) Логин и пароль от учётной записи и USB-токен.
4) Логин и пароль от учётной записи и смарт-карту.

9. Отметьте процесс, который носит название кибербуллинг.
1) Онлайн-спор, в который вовлечены определённое сообщество или группа в Интернете.
2) Травля, оскорбления и угрозы в условиях интернет-коммуникации.
3) Написание обидных комментариев к фотографиям, обвинение в непрофессионализме.

10. Какие данные хотят узнать фишеры?
1) Паспортные данные.
2) Номер школы.
3) Телефон.
4) Номер школьной карты.
5) Проверочный код от карты.
6) Пароль от учётной записи в социальной сети.
7) Пароль от онлайн-банкинга.
8) Номер банковской карты.
9) Логин и пароль от входа в дневник.
10) Логин и пароль от почты

Темы проектов:

1. Влияние социальных сетей на образ жизни современных подростков.
2. Сленг, используемый в социальных сетях.
3. Случайны ли орфографические ошибки при общении в социальных сетях и мессенджерах?
4. Группы в социальных сетях, опасные для психики детей и подростков.
5. Какие у меня есть права и обязанности в социальных сетях?

6. Реклама в сообществах социальных сетей.
7. Как стать блогером?

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.

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 несанкционирован-ного доступа к инфор-мации

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.

Приложение 2.

Требования к содержанию итоговых проектно-исследовательских работ

Критерии содержания текста проектно-исследовательской работы

1. Во введении сформулирована актуальность (личностная и социальная значимость) выбранной проблемы. Тема может быть переформулирована, но при этом четко определена, в необходимости исследования есть аргументы.
2. Правильно составлен научный аппарат работы: точность формулировки проблемы, четкость 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 ее 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 проведен 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 содержание работы, достаточная осведомленность в терминологической системе проблемы, отсутствие стилистических и речевых ошибок, соблюдение регламента.
2. Умение чѐтко 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 соответствующем 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 одноклассниками, проявление в ходе презентации коммуникабельности, благодарности и уважения по отношению к руководителю, консультантам, умение четко обозначить пути создания сетевого продукта.
7. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.