Принята

на заседании
педагогического совета
протокол № 1 от 31.08.2023

**Утверждена**

Директор Средней школы №1
_____ В.В. Ларина

приказ от 31.08.2023 № 214

Министерство просвещения Российской Федерации
Министерство образования Тульской области
муниципальное бюджетное образовательное учреждение
«Средняя школа №1 имени Героя Советского Союза Б.Н. Емельянова»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00CF68E4B22444074EF4B63BAC31C9C58D
Владелец: Ларина Валентина Васильевна
Действителен: с 17.10.2022 до 10.01.2024

# Рабочая программа
# учебного курса
# «Информационная безопасность»

(для 5-х классов)

Учитель информатики
Макарова Е.Н.

Щёкино, 2023

## Содержание

## ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» УЧЕБНОГО ПРЕДМЕТА «ИНФОРМАТИКА»

Целью модуля «Информационная безопасность» учебного предмета «Информатика» далее Программа является формирование у обучающихся навыков информационной культуры, профилактики негативных тенденций в информационной культуре; умение соблюдать нормы информационной этики и права; знание о роли информационных технологий и устройств в жизни людей; формирование навыка и умения безопасного и целесообразного поведения при работе с компьютерными программами и в сети Интернет; формирование активной позиции в получении знаний и умений выявлять информационную угрозу, определять степень её опасности, предвидеть последствия информационной угрозы и противостоять им; обеспечение условий для повышения защищённости детей от информационных рисков и угроз.

Задачи модуля Программы:

— дать представление о современном информационном обществе, информационной безопасности личности и государства;

— сформировать навыки ответственного и безопасного поведения в 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 организовывать информационный процесс);

— дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;

— познакомить со способами защиты от противоправных посягательств в Интернете защиты личных данных — дать представление о современном информационном обществе, информационной безопасности личности и государства;

— сформировать навыки ответственного и безопасного поведения в 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 организовывать информационный процесс);

— дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;
— познакомить со способами защиты от противоправных посягательств в Интернете защиты личных данных.

**Преимущество модуля Программы** заключается в том, что знание об информационной безопасности позволит успешно решить весь комплекс вышеперечисленных задач, являясь действенным средством обеспечения безопасности ребёнка в информационно-телекоммуникационной сети Интернет, воздействия интернета на формирование личности ребенка, его социализацию, защиты несовершеннолетних от негативной информации, размещенной в интернете.

В Программе специфика защиты информации, защиты ребёнка от негативной информации, размещённой в сети Интернет, защиты мобильных устройств удачно сочетаются с практическими занятиями, предполагая доступность освоения учебного материала всем возрастным категориям обучающихся.

Процесс реализации модуля Программы, опираясь на интегративный подход в обучении, позволяет планомерно реализовывать поставленную цель и последовательно решать задачи информационного воспитания обучающихся на протяжении трёх лет обучения в основной школе.

Программа реализуется в соответствии с Федеральным законом Российской Федерации от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (далее – Закон), который действует в интересах обучающихся образовательных организаций и утверждает:

- право образовательных организаций на самостоятельность в осуществлении образовательной деятельности и свободе в определении содержания образования, разработке и утверждении своих образовательных программ, выборе учебно-методического обеспечения, образовательных технологий по реализуемым ими образовательным программам (п. 1, п. 2, п. п. 6 п.3 ст.28 Закона);

- право педагогических работников на свободу выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания, а также право на творческую инициативу, разработку и применение авторских программ и методов обучения, и воспитания в пределах реализуемой образовательной программы, отдельного учебного предмета, курса, дисциплины (модуля) (п.п.2 и 3 п. 3 ст. 47 Закона);

**Нормативно-правовая база**

Программа разработана с учётом требований законов РФ:

- «Об образовании», Закон РФ от 10.07.1992 N 3266-1 (ред. от 10.07.2012);

- Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Указ президента РФ от 1 июня 2012 г. № 761 «О национальной стратегии действий в интересах детей на 2012 − 2017 годы»;
- «Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821-10.
- Указ Президента Российской Федерации от 06 декабря 2018 г. № 703 «О внесении изменений в Стратегию государственной национальной политики Российской Федерации на период до 2025 года, утверждённую Указом Президента Российской Федерации от 19 декабря 2012 г. № 1666».
- Указ Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года».
- Стратегия развития воспитания в Российской Федерации на период до 2025 года, утверждённая распоряжением Правительства Российской Федерации от 29 мая 2015 г. № 996-р.
- Программа разработана на основе требований федерального государственного образовательного стандарта основного общего образования (приказ Министерства образования и науки Российской Федерации от 17 декабря 2010 г. № 1897 «Об утверждении федерального государственного образовательного стандарта основного общего образования» (в редакции приказа Минобрнауки России от 31 декабря 2015 г. № 1577) к результатам освоения основной образовательной программы основного общего образования по учебному предмету «Информатика».

**Место учебного модуля в учебном плане**

Программа учебного курса рассчитана на 32 учебных часа, из них 18 часов — учебных занятий, 3 часа — проверка знаний, 9 часов — подготовка и защита учебных проектов, 2 часа — повторение.

## ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ МОДУЛЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» УЧЕБНОГО ПРЕДМЕТА «ИНФОРМАТИКА»

### Метапредметные результаты

*Межпредметные понятия*

В ходе изучения учебного модуля обучающиеся усовершенствуют опыт проектной деятельности и навыки работы с информацией, в том числе в текстовом, табличном виде, в 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 определённой 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 необходимое(ые) 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 определённого 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;
— 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 определённым 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:
— 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 её 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;
— 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 определённую 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 партнёра, 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 развёрнутый 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 партнёра 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 учётом 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 учётом 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.

## СОДЕРЖАНИЕ МОДУЛЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» УЧЕБНОГО ПРЕДМЕТА «ИНФОРМАТИКА»

Содержание модуля 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, подготовленные в ходе выполнения заданий.

## Тематическое планирование

| № п/п | Тема | Основное содержание | Количество часов |
|---|---|---|---|
| **Тема 1. «Безопасность общения»** | | | |
| 1 | Общение в социальных сетях и мессенджерах | Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент | 1 |
| 2 | С кем безопасно общаться в Интернете? | Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети | 1 |
| 3 | Пароли для аккаунтов социальных сетей | Сложные пароли. Онлайн генераторы паролей. Использование функции браузера по запоминанию паролей Правила хранения паролей. | 1 |
| 4 | Безопасный вход в аккаунты | Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта | 1 |
| 5 | Настройки конфиденциальности в социальных сетях | Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах | 1 |
| 6 | Публикация информации в социальных сетях | Персональные данные. Публикация личной информации | 1 |
| 7 | Кибербуллинг | Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать. Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. | 1 |
| 8 | Публичные аккаунты | Настройки приватности публичных страниц. Правила ведения публичных страниц | 1 |
| 9 | Фишинг | Фишинг как мошеннический приём. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах | 1 |
| 10 | Выполнение теста | Обсуждение тем индивидуальных и групповых | 1 |

| | | | |
|---|---|---|---|
| | | проектов | |
| 11 — 13 | Выполнение и защита индивидуальных и групповых проектов | | 3 |
| **Тема 2. «Безопасность устройств»** | | | |
| 1 | Что такое вредоносный код | Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов | 1 |
| 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 | 1 |
| 3 | Методы защиты от вредоносных программ | Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов | 1 |
| 4 | Распространение вредоносного кода для мобильных устройств | Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства | 1 |
| 5 | Выполнение теста | Обсуждение тем индивидуальных и групповых проектов | 1 |
| 6 – 8 | Выполнение и защита индивидуальных и групповых проектов | | 3 |
| **Тема 3 «Безопасность информации»** | | | |
| 1 | Социальная инженерия: распознать и избежать | Приёмы социальной инженерии. Правила безопасности при виртуальных контактах | 1 |
| 2 | Ложная информация в Интернете | Фейковые новости. Поддельные страницы | 1 |
| 3 | Безопасность при использовании платежных карт в Интернете | Транзакции и связанные с ними риски. Правила совершения онлайн-покупок. Безопасность банковских сервисов | 1 |

| | | | |
|---|---|---|---|
| 4 | Беспроводная технология связи | Уязвимости Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях | 1 |
| 5 | Резервное копирование данных | Безопасность личной информации. Создание резервных копий на различных устройствах | 1 |
| 6 | Выполнение теста. Обсуждение тем индивидуальных и групповых проектов | | 1 |
| 7 – 9 | Выполнение и защита индивидуальных и групповых проектов | | 3 |
| | Повторение, резерв | | 4 |
| | **Итого** | | **34** |

## РЕКОМЕНДУЕМАЯ УЧЕБНО – МЕТОДИЧЕСКАЯ ЛИТЕРАТУРА

1. Дневник Российского школьника "Российская символика. Интернет". - Москва: Высшая школа, 2009. - 228 с.
2. Солдатова, Г.В., Зотова Е.Ю., Чекалина А.И., Гостимская О.С. Пойманные одной сетью: социально-психологическое исследование представлений детей и взрослых об интернете / Под ред. Г.В. Солдатовой. — М., 2011. — 176 с.
3. Здоровье и безопасность подростков в сети Интернет. Комплект плакатов с методическим сопровождением. ФГОС. - М.: Учитель, 2018. - 821 с.
4. Макотрова, Г. В. Использование сети Интернет в познавательной деятельности старшеклассников: культурологический подход / Г.В. Макотрова. - М.: Флинта, 2014. - 689 с.
5. Мурсалиева, Г.Ш. Дети в сети: шлем безопасности ребенку в интернете / Г.Ш. Мурсалиева. - Москва: СИНТЕГ, 2016. - 320 с.
6. Чашин, А. Н. Борьба с правонарушениями в сети Интернет. Выпуск 1 / А.Н. Чашин. - М.: Дело и сервис, 2010. - 707 с.

### Интернет-ресурсы о безопасном Интернете

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».

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

**Приложение 2**

Ключи ответов к тесту по теме «Безопасность общения»

| **Номер задания** | **Правильный ответ** |
|---|---|
| 1 | 1-Е, 2-Д, 3-Г, 4-В, 5-А, 6-Б |
| 2 | онлайн-сервис в Интернете для общения и связи |
| 3 | |
| 4 | учётная запись пользователя в каком-либо сервисе |
| 5 | любимые места в городе;<br>твоё хобби;<br>любимые книги |
| 6 | приватность фотографий<br>приватность списка друзей<br>приватность персональных данных<br>приватность местоположения |
| 7 | ytrewq<br>drowssap<br>uiop<br>Mypassword<br>Ivan1968 |
| 8 | Логин и пароль от учётной записи и пароль из смс<br>Логин и пароль от учётной записи и USB-токен<br>Логин и пароль от учётной записи и смарт-карта |
| 9 | Травля, оскорбления и угрозы в условиях интернет-коммуникации |
| 10 | Паспортные данные<br>Телефон<br>Проверочный код от карты<br>Пароль от учётной записи в социальной сети<br>Пароль от онлайн-банкинга<br>Номер банковской карты<br>Логин и пароль от почты |

Ключи ответов к тесту по теме «Безопасность устройств»

| **Номер задания** | **Правильный ответ** |
|---|---|
| 1 | ворующие регистрационные данные;<br>дающие несанкционированный доступ к ключевым файлам различных программных продуктов;<br>использующие ресурсы компьютеров в интересах своего автора;<br>программы, проникающие в системные области данных и |

| | |
|---|---|
| | меняющие их;<br>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.<br>Ответами могут быть конкретные названия троянов, червей, приложений и ботнетов |
| 3 | Трояны распространяют люди, а вирусы распространяются самостоятельно.<br>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;<br>обновлять браузер, потому что в новых версиях исправляют уязвимости и недостатки предыдущих версий;<br>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:<br>Использовать антивирусное ПО.<br>Своевременно обновлять ПО, операционную систему, браузер и приложения.<br>Проверять приходящие файлы и ссылки перед скачиванием и открытием.<br>Проявлять интерес к информации от антивирусных компаний и экспертов по компьютерной безопасности.<br>Не проводить процедуру получения прав суперпользователя на устройствах.<br>Не скачивать файлы с подозрительных источников.<br>Обращать внимание на расширение загружаемого файла.<br>Воздержаться от загрузки пиратской версии программ, а скачивать файлы с официального сайта производителя. |

| | |
|---|---|
| | Не скачивать приложение в комплекте с дополнительным ПО.<br>Читать отзывы и советоваться с родителями и друзьями |
| 11 | Вирусы<br>Черви<br>Трояны<br>Бэкдоры<br>Руткиты |
| 12 | регулярное обновление браузера<br>регулярное обновление операционной системы<br>регулярное обновление антивирусной базы<br>проверка адресов сайтов<br>отказ от перехода по ссылкам из всплывающих окон<br>использование диспетчера задач для закрытия браузера в случае заражения<br>загрузка ПО только с официальных сайтов-разработчиков<br>выбор зарекомендовавших себя антивирусных программ<br>установка только лицензионных версий ПО<br>установка проактивного и поведенческого анализа в антивирусной базе<br>проверка почтовых сообщений и их вложений<br>полное сканирование компьютера и подключаемых устройств не реже 1раза в неделю |

Ключи ответов к тесту по теме «Безопасность устройств»

| **Номер задания** | **Правильный ответ** |
|---|---|
| 1 | 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 |
| 2 | Политика<br>Реклама и продвижение товаров<br>Торговля<br>Маркетинг<br>Артистическая сфера |
| 3 | 3, 4, 5<br>Возможный ответ: Википедия в сочетании в другими |

<table>
<tr><td></td><td>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;<br>общественный транспорт;<br>поликлиника;<br>ВУЗ</td></tr>
<tr><td>6</td><td>WEP</td></tr>
<tr><td>7</td><td>замочек рядом со значком Wi-Fi<br>Авторизация в Сети<br>Wi-Fi с паролем доступа</td></tr>
<tr><td>8</td><td>операционная система обновлена<br>версия браузера обновлена<br>двухфакторная онлайн-транзакция<br>свой компьютер<br>обновлённый антивирус, установленный на устройстве, с которого производится транзакция<br>правильный адрес в адресной строке<br>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 порчи жёсткого диска<br>защита от физической порчи флеш-карты</td><td>возможность использования и сохранения последней версии реферата, доклада или других рабочих документов<br><br>хранение ценных файлов и данных на любом устройстве</td><td>защита информации от вредоносного ПО<br><br>хранение первоначальной версии операционной системы, не заражённой вредоносными программами</td></tr>
</table></td></tr>
<tr><td>10</td><td>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</td></tr>
</table>

**Приложение 3**

## ГЛОССАРИЙ

Аватар — графическое представление пользователя.

Аккаунт социальной сети — это учётная запись, личная страница пользователя в социальной сети.

Антивирусная программа (антивирус) — это программное обеспечение, защищающее устройство от действий и проникновения вредоносного кода.

Аутентификация — это процедура проверки подлинности личности для входа в аккаунт.

Блог — это интернет-страница, основное содержимое которой — регулярно добавляемые записи, содержащие текст, изображения или мультимедиа.

Блогер — это человек, который ведёт свой блог в Интернете (онлайн-журнал, youtube-канал и др.).

Бот — вредоносное программное обеспечение, призванное выполнять любые ко-манды, полученные от командного центра.

Ботнет — это сеть устройств, которые по команде злоумышленника могут про-изводить атаки на различные ресурсы, рассылать спам, производить любые другие опасные действия.

Браузер — это программа для загрузки интернет-страниц.

Буллинг (от англ. Bully — хулиган) — это избиение или психологическая травля одного человека другим.

Бэкдор — это тип трояна, предоставляющий своему хозяину возможность удалённого управления компьютером жертвы.

Вирус — это самовоспроизводящийся вредоносный код.

Внешний носитель — это устройство для хранения, накапливания и передачи информации.

Гаджет — это портативное техническое устройство (планшет, смартфон и т. д.).

Домен — уникальный адрес (имя) сайта в Интернете, состоящий из набора символов и цифр.

Идентифицировать — определить полное соответствие предмета или человека другому предмету или человеку по определённым признакам.

Инверсия — это набор русского словосочетания при включённой английской раскладке клавиатуры.

Инсталляция — это процесс установки программного обеспечения.

Интернет-троллинг — это форма провокации или издевательства в интернет-мире, использующаяся как одиночными участниками, так и группой.

Интерфейс — это набор инструментов для взаимодействия человека и компьютерной техники.

Исполняемый файл — это код, который начнёт выполняться на компьютере пользователя после запуска.

Кибербуллинг (кибертравля, интернет-травля) — это угрозы, оскорбления или травля, совершаемые в течение длительного времени через Интернет.

Киберпреступники — это злоумышленники, совершающие преступления с помощью цифровых технологий.

Кибersталкинг — перенос явления «сталкинга» в Интернет.

Конфиденциальность — это предотвращение разглашения или утечки какой-либо информации, в том числе личной.

Логин — это имя пользователя, использованное для регистрации на сайте.

Макросы — это алгоритмы, чаще всего использующиеся в офисных приложениях для автоматизации каких-то процессов.

Мессенджер — это программа (приложение) для мгновенного обмена сообщения-ми через Интернет. В качестве сообщений мессенджеры могут использовать текст, картинки, видео, некоторые приложения поддерживают передачу файлов любого формата.

Мобильный Интернет — технология подключения к Интернету через мобильное устройство (смартфон, планшет и др.).

Нигерийские письма — это вид интернет-мошенничества, связанный с массовой рассылкой писем по электронной почте.

Никнейм — это псевдоним, используемый пользователем в Интернете (в блогах, чатах или играх).

Онлайн-банкинг — это технология дистанционного банковского обслуживания.

Операционная система — это комплекс программ, связанных между собой и предназначенных для управления ресурсами устройства.

Открытый доступ в социальной сети — это доступ в режиме реального времени к пользовательскому контенту.

Паблик — это страница социальной сети, в которой публикуется определённый тематический контент.

Пароль — это определённый набор знаков, необходимый для подтверждения личности.

Патч — это программа, содержащая улучшенный или обновлённый код для операционной системы или приложения.

Персональные данные — это любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных) (согласно п. 1 ст. 3 Федерального закона от 27 июля 2006 года № 152-ФЗ).

Платёжная карта — это инструмент, позволяющий держателю карты производить оплату с помощью электронного перевода.

Платёжная система — это сервис для перевода денег или иных средств, их заменяющих.

Пользовательский контент — это уникальный информационный материал, который создаётся потребителями определённого ресурса.

Поп-ап — это всплывающее окно на экране компьютера в результате какого-либо действия пользователя.

Приватная переписка — это обмен личными сообщениями, которые доступны только отправителю и получателю.

Приватность — это неприкосновенность частной жизни человека.

Псевдоним — это вымышленное имя.

Расширение файла — это несколько букв после точки в конце названия любого файла, обозначающие его формат.

Режим «инкогнито» — это функция браузера, позволяющая повысить анонимность в Интернете путём прекращения процессов сохранения истории просмотренных страниц, загрузки файлов и т. д.

Репутация — это общественное мнение, сложившееся о ком-либо или о чём-либо (например, репутация компании) на основании его качеств, достоинств, недостатков и т. п.

Роутер — это прибор, позволяющий настроить рабочую или домашнюю сеть из нескольких устройств (компьютеров, планшетов и др.).

Рунет — это определённая часть Интернета с контентом преимущественно на русском языке.

Руткиты — это класс вредоносных программ, скрытно действующих в заражённой системе и обладающих специальными средствами, затрудняющими их обнаружение системами безопасности.

Скриншот — это изображение, полученное компьютером или мобильным устройством, показывающее то, что видит пользователь на экране монитора.

Скрипт — это программа или небольшой кусок кода, позволяющий автоматизировать какое-то действие.

Смарт-карты (от англ. smart card — умная карта) — это пластиковые кар-ты со встроенной микросхемой, предназначенные для одно- и двухфакторной аутентификации пользователей, хранения ключевой информации и т. д.

СМИ (средства массовой информации) — совокупность органов публичной передачи информации с помощью технических средств.
Софт — это собирательное название программного обеспечения.
Социальная инженерия — это метод управления действиями человека без использования технических средств.
Социальная сеть — это специально созданный онлайн-сервис или веб-сайт, позволяющий людям и организациям общаться и обмениваться информацией.
Спам — это массовые незапрашиваемые рассылки сообщений через средства электронной коммуникации.
Сталкинг (от англ. stalking — облава) — это навязчивое внимание к человеку со стороны другого человека или группы лиц.
Токен — это устройство, предназначенное для обеспечения информационной безопасности, безопасного удалённого доступа к информационным ресурсам, идентификации владельца и т. д.
Транзакция — это операция перевода или снятия средств с банковской карты.
Тролль — это пользователь, который провоцирует и оскорбляет своими сообщениями других пользователей на форумах, в социальных сетях.
Утилита — это вспомогательная компьютерная программа в составе общего программного обеспечения, созданная для выполнения каких-либо типовых задач, в основном связанных с работой операционной системы.
Уязвимость — это ошибка в коде, не исправленная создателем.
Фанаты — это ярые поклонники чего-либо или кого-либо.
Фейковая новость — это преднамеренное распространение дезинформации в виртуальных медиа и традиционных СМИ для введения в заблуждение читателей.
Фишеры — это интернет-мошенники, занимающиеся фишингом.
Фишинг — это форма киберпреступности, основанная на методах социальной инженерии. Предполагает кражу конфиденциальных данных с компьютера пользователя и использование этих данных для получения его денег.
Целевая атака — это непрерывный процесс несанкционированной активности в инфраструктуре атакуемой системы, удалённо управляемый в реальном времени вручную.
Чекин (от англ. to check in — отметиться по прибытии) — это сообщение, отправляемое пользователем в социальных сетях, о его местонахождении.
Эмулятор — это программа, позволяющая воспроизводить программы на операционной системе, для которой данные программы разработаны не были.

Jailbreak — это процедура получения прав суперпользователя на устройствах IOS.

Steam — это крупнейшая игровая платформа, сочетающая в себе функции он-лайн-магазина, социальной сети для игроков и библиотеки игр.

VPN (англ. Virtual Private Network) — это виртуальная частная сеть, которая используется для предоставления сотрудникам удалённого доступа к корпоративной сети через Интернет.

WEP (Wired Equivalent Privacy) — это алгоритм для обеспечения безопасности сетей Wi-Fi.

Wi-Fi — один из форматов передачи цифровых данных без использования проводов.

**Приложение 4**

## 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.