цифровой диктант.рф

Методические рекомендации по Цифровой Грамотности

1. **Методические рекомендации «Введение в цифровую грамотность»**

Методическая рекомендация содержит базовые правила кибербезопасности для защиты устройств и личных данных в интернете. В ней рассматриваются вопросы безопасного подключения к общественным Wi-Fi сетям, отписки от нежелательных рекламных рассылок и распознавания мошеннических объявлений при поиске работы. Также приводятся 10 признаков, указывающих на то, что вам пишет или звонит мошенник. В заключение даны советы по резервному копированию данных и удалению старых приложений.
Подробнее

2. **Методическое пособие «Риски в цифровой среде»**

Методическое пособие посвящено проблеме цифровых рисков, с которыми сталкиваются дети разных возрастов (дошкольники, младшие школьники и подростки). В пособии рассматриваются причины цифровых рисков, связанные с психологическими особенностями каждого возраста, а также представлены современные инструменты для диагностики этих рисков. Предлагаются рекомендации для родителей и педагогов по профилактике и коррекции цифровых рисков в разные периоды детства.
Подробнее

3. **Гид по финансовой грамотности**

В гиде рассматриваются основные возможности, которые интернет предоставляет для совершения покупок, платежей и управления деньгами, а также связанные с ними угрозы и способы защиты от наиболее типичных опасностей. Брошюра охватывает вопросы совершения обычных платежей, покупок в интернет-магазинах, безопасности при использовании мобильных сервисов и семейной финансовой безопасности. Особое внимание уделено различным видам интернет-мошенничеств и вымогательств, сопровождающих финансовую онлайн-жизнь

пользователей. Руководство также содержит информацию об электронных деньгах, онлайн-аукционах, безопасности персональных данных и финансовых аспектах использования интернета детьми.
Подробнее

4. **Занятие для обучающихся 2-6 классов по теме: «Вредоносные программы»**

Методическое пособие представляет собой разработку внеурочного занятия для учеников 2-6 классов, целью которого является знакомство с различными видами компьютерных вирусов, способами их распространения, методами профилактики и борьбы с ними. В файле раскрываются понятия вредоносных программ (вирусы, трояны и другие), способы их проникновения на устройства, а также методы защиты, включая использование антивирусного программного обеспечения и безопасное поведение в интернете.
Подробнее

5. **Пособие «Безопасность в интернете»**

Это методическое пособие разработано для проведения внеурочных занятий с учениками 7-11 классов. Его основная цель – повышение уровня информационной безопасности школьников путем формирования навыков ответственного и безопасного поведения в интернете.
В пособии рассматриваются следующие вопросы:

- ➢ Что такое интернет-безопасность и почему она важна.
- ➢ Как распознавать безопасные и небезопасные онлайн-практики.
- ➢ Какие действия предпринимать при столкновении с неприятными или опасными ситуациями в сети.
- ➢ Правила безопасного общения и использования интернет-ресурсов.

В структуру занятия включены обсуждения, упражнения и ролевые игры, направленные на развитие критического мышления, умения анализировать информацию и принимать взвешенные решения в онлайн-среде. Пособие также содержит приложения с примерами фишинговых сообщений и сценариями опасных ситуаций в интернете.
Подробнее

6. **Методические рекомендации «Конфиденциальность данных»**

Эти материалы представляют собой методическую разработку внеурочного занятия для учеников 7-11 классов, посвященную формированию знаний и навыков безопасного поведения в интернете, а также ответственного отношения к персональным данным.

Основные темы занятия:

- ➢ Что такое личные данные и конфиденциальность.
- ➢ Риски, связанные с незащищенной личной информацией (кража идентичности, мошенничество).
- ➢ Способы защиты личной информации: использование сложных паролей, осторожность при общении в интернете.

В структуру занятия включены:

- ➢ Обсуждение и групповая работа.
- ➢ Интерактивное упражнение «Реальный сценарий» с анализом различных ситуаций, связанных с конфиденциальностью данных.
- ➢ Создание проектов по защите данных.

В качестве домашнего задания предлагается семейное обсуждение темы конфиденциальности данных и аудит безопасности своих онлайн-аккаунтов.

Цель занятия – научить школьников осознанно относиться к своей личной информации в интернете и принимать меры для ее защиты.

Подробнее

7. **Пособие «Компьютерная зависимость»**

Эта методическая разработка представляет собой внеурочное занятие для учащихся 7-11 классов, направленное на привлечение внимания к проблеме компьютерной зависимости. Цель занятия – расширить представления учеников о пользе и вреде современных технических средств.

В ходе занятия планируется:

- ➢ Определить, что такое компьютерная зависимость и как она влияет на жизнь.
- ➢ Обсудить важность умения контролировать время, проведенное за компьютером.
- ➢ Научиться выявлять здоровые и нездоровые привычки в использовании компьютеров и других устройств.

В материалах рассматриваются причины и факторы риска развития зависимости, её симптомы и последствия, а также стратегии управления и профилактики. В структуру занятия включены обсуждения, групповая работа и рефлексия. Предлагаются задания для самостоятельной работы после занятия, направленные на самонаблюдение, распространение знаний и организацию «цифрового детокса».
Подробнее

8. **Пособие «12 правил интернет-безопасности»**

Рекомендации по безопасному поведению в интернете, включая проверку посещаемых сайтов, использование сложных паролей и осторожность при общении онлайн
Подробнее

9. **Пособие «Как не стать жертвой интернет-мошенников»**

В пособии описываются такие виды мошенничества, как финансовые пирамиды, брачные аферы, фальшивые предложения работы, «нигерийские письма» и опасные сообщения с вредоносным содержимым. Мошенники используют различные методы, чтобы втереться в доверие и выманить деньги или личные данные пользователей.
Подробнее

10. **Пособие «Кибербуллинг»**

Методичка рассказывает о кибербуллинге, рассматривая его как серьезную контентную угрозу, влияющую на психику и социализацию человека, особенно в условиях размытости границ между онлайн и офлайн мирами. В статье перечислены основные формы травли в сети, включая оскорбления, домогательства, распространение слухов, использование чужого имени, разглашение личной информации, распространение компрометирующих сведений, социальную изоляцию и прямые угрозы.
Подробнее

11. **Пособие «Как защитить свои данные»**

Пособие объясняет важность защиты личной информации от угроз, которые могут привести к краже денег или использованию данных в мошеннических схемах. В пособии рассматриваются распространённые

угрозы, такие как кража данных банковских карт и личной информации, а также отслеживание профилей в социальных сетях.
Подробнее

12. **Методическая рекомендация «Безопасность в Интернете»**

Методическая рекомендация посвящена безопасному использованию социальных сетей детьми. В ней содержатся практические советы для родителей по настройке приватности и ограничению контента в популярных социальных сетях, таких как TikTok, ВКонтакте. Рекомендации включают установку приватного аккаунта, ограничение неподходящего контента, контроль времени использования приложений, блокировку нежелательных пользователей. Главная цель – подготовить детей к безопасному и продуктивному использованию технологий.
Подробнее

13. **Пособие «Обучаем близких цифровой грамотности»**

Пособие предлагает способы помощи тем, кто не владеет навыками поиска информации в интернете, опираясь на данные опроса, согласно которому большинство пользователей осваивают цифровой мир самостоятельно или с помощью друзей. В материале рекомендуется делиться знаниями о технологиях с близкими, особенно с родителями, помогая им устанавливать программы и разбираться с устройствами.
Подробнее

14. **Методические рекомендации «Как сделать интернет безопасным для ребенка?»**

Рекомендации включают создание отдельной учетной записи для ребенка с ограниченными правами, активацию функций родительского контроля и безопасного поиска, а также установку детского поисковика. Важным аспектом является установление доверительных отношений с ребенком, обучение критическому отношению к информации в сети, правилам конфиденциальности в социальных сетях и способам реагирования на киберагрессию.
Подробнее

15. Статья «50 правил безопасности в интернете»

Статья включает в себя советы по защите личной информации, безопасному использованию Wi-Fi, созданию надежных паролей, установке антивирусного программного обеспечения, осторожности при переходе по ссылкам и открытии файлов, а также рекомендации по безопасному поведению в социальных сетях и мессенджерах. Статья также затрагивает вопросы защиты детей в интернете и резервного копирования данных.

Подробнее

Подборка каналов для изучения Цифровой Грамотности

1. **Цифровой Диктант**

Цифровой Диктант – Всероссийская акция, признанная самой масштабной в России проверкой знаний в области цифровой грамотности.

Акция дает возможность пользователям не только узнать свой уровень цифровых компетенций, но и пройти работу над ошибками, а также сформировать свою личную стратегию развития недостающих знаний и навыков.

Подробнее

2. **ЦИФРАтека**

Портал Альянса по защите детей в цифровой среде, на котором собрана информация об угрозах в Интернете и советы, как с ними справляться.

Подробнее

3. **Кибердом**

Площадка «Кибердом» – это первое в мире мультифункциональное пространство, полностью посвященное кибербезопасности. На площади 2 400 кв. м расположились несколько локаций, ориентированных на мероприятия разного уровня – от киберконференций и гибридных ивентов «под ключ» до неформальных переговоров и онлайн-эфиров с AR.

Подробнее

4. **РОЦИТ**

Общественная организация, объединяющая активных интернет-пользователей России. Поддерживает образовательные проекты в области IT и цифровой грамотности, представляет актуальные исследования интернет-пользования , защищает интересы пользователей и специалистов интернет-сферы на государственном уровне и представителями бизнеса, развивает культуру потребления интернета среди граждан.

Подробнее

5. **Курс «Компьютерная грамотность для детей» в детской школе программирования «Пиксель»**

Преподаватели школы «Пиксель» уверены, что быть с компьютером на «ты» необходимо каждому ребенку. Курс рассчитан на детей 7-10 лет.

Полученные знания пригодятся ребятам и в учебе, и в повседневной жизни. При просмотре видео-уроков, выложенных канале школы, они познакомятся с понятием «операционная система», научатся быстро печатать, пользоваться Google Документами, Google Презентациями и Google Таблицами, защищать проекты и выступать перед аудиторией. В курс входит большой блок тем, посвященный безопасности в сети: как не попасться на удочку мошенников, уберечься от кибератак, защитить себя при общении online.

Подробнее

6. **Информационно-обучающие видеоролики для повышения цифровой грамотности от Академии Минпросвещения России.**

Полезные материалы по компьютерной грамотности есть и на других видео-хостингах, например, на Rutube. На видео-занятиях, разработанных Академией Минпросвещения России, детям от 10 лет объясняют:

- ➢ как придумать и запомнить сложный пароль;
- ➢ как обеспечить безопасность смартфона;
- ➢ как пользоваться двухфакторной аутентификацией для защиты страниц в соцсетях;
- ➢ какие опасности таит бесплатный Wi-Fi;
- ➢ как защититься от ненужной информации по e-mail;
- ➢ нужно ли создавать резервные копии.

Подробнее

7. **Проект «Цифровой ликбез»**

Просветительский проект, который поможет повысить цифровую грамотность и узнать больше о кибербезопасности в сети. Видеоролики для детей и взрослых от ведущих цифровых компаний-лидеров: VK, Благотворительный фонд Сбербанка «Вклад в будущее», СКБ Контур, «Лаборатория Касперского», Авито.

Подробнее

8. **Курс «Специалист по информационной безопасности»**

На курсе вы погрузитесь в специфику профессии и попробуете решить реальные задачи специалиста.

На курсе вы узнаете:

- ➢ Чем занимается специалист по информбезопасности (Изучите особенности профессии и поймёте, подходит ли она вам);
- ➢ Какие специализации существуют (Узнаете, какие возможности для развития есть внутри профессии);
- ➢ Какие методы и инструменты использует специалист (Познакомитесь с инструментами и самостоятельно решите реальные задачи специалиста);
- ➢ Как строить карьеру и какие навыки развивать (Поймёте, как начать свой путь в профессии и какие навыки будут необходимы на старте).

Подробнее