**Основы цифровой безопасности: как научить школьников защищать личные данные в интернете**

Автор: **Оразбай Зарина Әзімханқызы**

Должность: Учитель информатики

Дата: **10.02.2025**

1. Введение
2. Основная часть

2.1. Что такое цифровая безопасность
2.2. Основные угрозы для школьников в интернете
2.3. Практические методы обучения цифровой безопасности
2.4. Примеры уроков и проектов

1. Заключение
2. Список литературы

В современном мире интернет стал неотъемлемой частью повседневной жизни, влияя на различные аспекты деятельности человека — от образования до развлечений. Особенное внимание в этом контексте следует уделить школьникам, которые с раннего возраста активно используют цифровые технологии. Интернет предоставляет безграничные возможности для получения знаний, общения и творчества, но вместе с тем он становится и источником различных угроз, таких как утечка личных данных, кибербуллинг, фишинг и вредоносные программы.

Школьники часто не осознают возможные риски, связанные с их активностью в интернете. Они размещают личную информацию в социальных сетях, используют слабые пароли и переходят по подозрительным ссылкам, что делает их уязвимыми для злоумышленников. Это вызывает необходимость систематического обучения основам цифровой безопасности, чтобы подготовить школьников к безопасному использованию цифровых технологий.

Цель данной статьи — показать важность формирования у школьников навыков цифровой безопасности, описать основные угрозы, которые их подстерегают, и предложить эффективные методы обучения. Это позволит педагогам внедрять системный подход в образовательный процесс, способствуя развитию цифровой грамотности у детей.

**2.1. Что такое цифровая безопасность**

Цифровая безопасность — это совокупность мер и правил, которые позволяют пользователям защищать свои данные, устройства и онлайн-активность от несанкционированного доступа, мошенничества и других киберугроз. Для школьников цифровая безопасность особенно важна, так как они являются активными пользователями социальных сетей, игровых платформ и образовательных онлайн-ресурсов.

Основные аспекты цифровой безопасности включают:

* Защиту персональных данных (логины, пароли, адреса, банковская информация);
* Безопасное использование социальных сетей;
* Защиту устройств от вирусов и вредоносных программ;
* Критическое восприятие информации в интернете;
* Умение избегать взаимодействия с подозрительными ссылками и файлами.

**2.2. Основные угрозы для школьников в интернете**

Школьники часто становятся мишенью различных киберугроз из-за своей неопытности. Среди наиболее распространённых угроз:

1. **Кибербуллинг** — оскорбления, травля или унижение в интернете.
2. **Фишинг** — попытки выманить у пользователя личные данные, например, пароли или банковские реквизиты, через поддельные сайты или письма.
3. **Утечка данных** — когда пользователь делится личной информацией в соцсетях, её могут использовать злоумышленники.
4. **Мошенничество** — предложения «выиграть приз» или «быстро заработать» в обмен на предоплату или данные банковской карты.
5. **Вредоносные программы** — вирусы и шпионское ПО, которые крадут данные или блокируют устройства.

**2.3. Практические методы обучения цифровой безопасности**

Обучение школьников должно быть интерактивным и включать как теорию, так и практику. Вот основные подходы:

1. **Разъяснение понятий**: Учителю важно объяснить учащимся, что такое персональные данные, почему их нельзя распространять, и как защитить свои устройства.
2. **Реальные примеры**: Показывайте случаи киберугроз, близкие к реальности. Например, демонстрируйте поддельные письма фишинга или рассказывайте истории о кибербуллинге.
3. **Практические занятия**:
	* Создание надёжных паролей и проверка их стойкости через специальные онлайн-сервисы.
	* Определение фейковых страниц или писем в интернете.
	* Настройка конфиденциальности в социальных сетях.
4. **Ролевые игры**: Проведение игр, где ученики должны распознать угрозу и предложить способы защиты. Например, разыгрывание сценариев фишинговой атаки или взлома профиля в соцсети.
5. **Использование цифровых ресурсов**: Привлекайте современные платформы, такие как Google for Education, Яндекс.Учебник или специализированные сайты для обучения кибербезопасности (например, «Сетевичок»). Также полезно рекомендовать мобильные приложения для проверки безопасности устройств и аккаунтов.
6. **Дискуссии и дебаты**: Организуйте обсуждения на тему: "Что важнее — конфиденциальность или удобство в интернете?" Это помогает школьникам развивать критическое мышление и формировать осознанный подход к использованию технологий.

**2.4. Примеры уроков и проектов**

1. **Тема урока: «Как создать надёжный пароль?»**
	* Цель: Научить школьников придумывать сложные пароли.
	* Задание: Используя правила (длина пароля, использование букв, цифр, символов), создать 3 варианта паролей и протестировать их на сайте проверки стойкости.
2. **Проект: «Профиль безопасности в интернете»**
	* Учащиеся анализируют свои профили в социальных сетях, выявляют открытые данные и предлагают способы их защиты.
3. **Квест: «Спаси данные»**
	* Серия заданий с имитацией киберугроз, где школьники должны применять полученные знания для защиты личных данных.

Цифровая безопасность — это неотъемлемая часть современной жизни, особенно для школьников, которые активно используют интернет. В условиях стремительного роста киберугроз важно научить детей распознавать опасности и защищать свои данные. Обучение цифровой безопасности должно быть включено в образовательный процесс как неотъемлемая его часть.

Реализация систематического подхода к обучению школьников основам цифровой безопасности позволяет не только формировать у них практические навыки, но и развивать критическое мышление и ответственность за свои действия в интернете. Интерактивные методы, реальные примеры и проектная деятельность создают прочную основу для осознанного использования цифровых технологий.

Учителя играют ключевую роль в этом процессе, выступая проводниками знаний и наставниками для школьников. Подготовив детей к встрече с цифровыми вызовами, мы способствуем формированию безопасного и защищён

Обучение цифровой безопасности — это важная часть образовательного процесса в современном мире. Учителя информатики играют ключевую роль в формировании у школьников навыков безопасного поведения в интернете. Использование интерактивных методов, реальных примеров и проектной работы помогает учащимся осознать значимость защиты личных данных и применять полученные знания на практике.

Интернет — это не только источник информации, но и пространство потенциальных угроз. Чем раньше дети научатся распознавать опасности и защищать себя, тем безопаснее будет их цифровое будущее.

**Список литературы**

1. Лукьянов, А.В. Цифровая безопасность в школе. — М.: Просвещение, 2020.
2. Официальный сайт «Сетевичок»: [https://сетевичок.рф](https://xn--b1afankxqj2c.xn--p1ai/).
3. Материалы курса Google for Education: [https://edu.google.com](https://edu.google.com/).
4. Федеральные рекомендации по информационной безопасности: [https://edu.gov.ru](https://edu.gov.ru/).
5. Поляков, И.И. Основы информационной безопасности. — СПб.: Питер, 2019.