Неофитова Наталия Николаевна
учитель
МБОУ «Янтиковская СОШ
имени Героя Советского Союза П.Х. Бухтулова»
с. Янтиково, Чувашская Республика

ЦИФРОВОЙ МИР: УЧИМСЯ ЗАЩИЩАТЬ СВОИ ДАННЫЕ

Аннотация: *автор статьи отмечает, что сегодня цифровые технологии пронизывают все сферы жизни. Школьники активно пользуются интернетом – учатся, общаются, играют, создают контент. Но вместе с возможностями приходят и риски: утечка персональных данных, взлом аккаунтов, кибермошенничество. Именно поэтому обучение основам цифровой безопасности в школе – не опция, а необходимость.*

Ключевые слова: *кибербезопасность, защита данных, пароли, антивирусное ПО, безопасное поведение в интернете, шифрование, личные устройства, фишинг, кибермошенничество, цифровая безопасность.*

В современном мире информация – один из самых ценных ресурсов. С каждым днём мы всё больше полагаемся на цифровые технологии: храним личные данные в облаке, ведём онлайн-дневники, совершаем покупки в интернете. Но вместе с удобством приходят и риски – угроза взлома, кражи личных данных и мошенничества. Поэтому важно с раннего возраста учить детей основам кибербезопасности.

Основы цифровой безопасности нужно осваивать так же, как чтение и письмо.

Почему эту тему важно изучать в школе?

Ранняя профилактика рисков для школьников в цифровом мире – это комплекс мер, направленных на формирование безопасного поведения в интернете, развитие критического мышления и устойчивости к негативному влиянию он-

лайн-среды. Она включает просветительскую работу с детьми, родителями и педагогами, использование технических средств защиты и психолого-педагогическую поддержку.

Цель ранней профилактики – не только минимизировать риски, но и сформировать у школьников осознанное и безопасное отношение к цифровому миру. Дети становятся жертвами мошенников: взлом аккаунтов в играх (потеря виртуальных ценностей); кража персональных данных через фишинговые ссылки; кибербуллинг из-за утечки личной информации.

Основные направления профилактики.

1. *Информирование о рисках.* Школьникам надо объяснять, что в интернете важно сохранять приватность (не публиковать личные данные, геолокацию), не общаться с незнакомцами, не передавать пароли и конфиденциальную информацию, а также обсуждать риски кибербуллинга, мошенничества, вовлечения в опасные группы или сообщества.

2. *Развитие цифровой грамотности.* Следует учить детей критически оценивать информацию, различать достоверные и недостоверные источники, безопасно использовать соцсети и мессенджеры. Для младших школьников хорошо проводить игровые занятия, для подростков – тренинги.

3. *Доверительное общение в семье.* Родители и педагоги должны выстраивать открытые отношения, чтобы ребёнок не боялся делиться проблемами, связанными с интернетом. Полезно обсуждать онлайн-активность, но избегать чрезмерного контроля и запретов, которые могут привести к потере доверия.

4. *Использование технических средств защиты.* Необходимо применять функции родительского контроля (ограничение времени в интернете, блокировка нежелательного контента), антивирусы, настройки приватности в устройствах и приложениях. Например, программа вроде Kaspersky Safe Kids позволяет управлять доступом к сайтам и отслеживать активность.

5. *Работа с родителями.* Целесообразно проводить родительские собрания, консультации, дискуссии, где обсуждаются методы профилактики, технические инструменты и роль семьи в формировании безопасного поведения и рассказать

родителям о службах поддержки и организациях, куда можно обратиться в случае проблем.

6. *Психолого-педагогическая поддержка в школе.* Педагогам и психологам полезно проводить занятия, направленные на развитие навыков общения, самоконтроля, преодоления трудностей. Это поможет снизить риск интернет-зависимости и деструктивного поведения.

7. *Создание позитивной онлайн-среды.* Полезно вовлекать школьников в разработку и модерирование позитивно ориентированных интернет-проектов (например, школьных порталов или сообществ), способствующих формированию ответственного отношения к цифровой среде.

Методы профилактики адаптируются под возрастные особенности школьников. Совместная работа школы, родителей и специалистов повышает эффективность мер. Важно формировать устойчивые привычки у школьников в цифровом мире.

Ключевые привычки, которые важно сформировать.

1. *Гигиена цифрового пространства:* регулярное обновление паролей; использование двухфакторной аутентификации; очистка истории браузера и кэша; проверка разрешений приложений.

2. *Безопасная коммуникация:* не делиться личными данными с незнакомцами; критически оценивать запросы на дружбу и сообщения; использовать настройки приватности в соцсетях; сообщать взрослым о подозрительных контактах.

3. *Контроль времени и внимания:* соблюдение лимитов на использование гаджетов; регулярные перерывы при работе за экраном; отключение ненужных уведомлений; «цифровые выходные» или периоды без гаджетов.

4. *Критическое мышление в цифровой среде:* проверка источников информации перед её использованием; распознавание фейков и манипулятивных техник; осознанное потребление контента (отписка от токсичных каналов); рефлексия над собственными эмоциями от онлайн-взаимодействий.

5. *Ответственность за цифровой след:* обдумывание последствий публикаций; уважение к авторским правам (не копировать без ссылки); вежливое и корректное общение в сети; умение удалять нежелательный контент о себе.

6. *Кибербезопасность:* не открывать подозрительные ссылки и вложения; использование антивирусов и брандмауэров; резервное копирование важных данных; осторожность при онлайн-платежах.

Подготовка школьников к цифровому будущему – это системная работа по формированию комплекса компетенций, позволяющих уверенно, безопасно и продуктивно существовать в высокотехнологичной среде завтрашнего дня.

Навыки цифровой коммуникации показывают эффективное использование мессенджеров и платформ для видеозвонков; деловой онлайн-этикет; уважительное общение в сети, профилактика кибербуллинга.

Изучая цифровую этику и ответственность, школьники учатся уважать авторские права; управлять цифровой идентичностью; понимают о последствиях онлайн-действий.

Воспитание цифровой ответственности у школьников – это процесс формирования осознанного отношения к собственным действиям в цифровой среде, понимания их последствий и готовности нести за них ответственность, умение уважать чужую приватность и не распространять чужие данные.

Методы воспитания:

− диалоги и дискуссии – разбор реальных кейсов, обсуждение последствий необдуманных действий;

− ролевые игры – отработка ситуаций с этическими дилеммами в цифровой среде;

− проектная деятельность – создание позитивного контента, образовательных материалов о цифровой безопасности;

− наставничество – старшие ученики помогают младшим осваивать правила цифрового поведения;

− правила цифрового кодекса – совместная разработка школьных норм онлайн-поведения;

− примеры из медиа – анализ публичных инцидентов, связанных с нарушением цифровой этики.

Школа должна стать тем местом, где ученик не просто получает информацию, но и учится защищать себя в цифровом мире. Ведь безопасность – это не страх, а осознанность и компетентность.

Список литературы

1. Концепция информационной безопасности детей в Российской Федерации (утверждена распоряжением Правительства РФ от 28.04.2023 №1105-р) // Официальный интернет-портал правовой информации [Электронный ресурс]. – Режим доступа: http://publication.pravo.gov.ru/document/0001202305050026 (дата обращения: 15.01.2026).

2. Лига безопасного Интернета [Электронный ресурс]. – Режим доступа: https://alice.yandex.ru/chat/019be235-ae8b-4000-b897–45d51d12165d/?utm_source=yandex&utm_campaign=serp_header_oknyx&utm_medium=interface (дата обращения: 15.01.2026).

3. Сустина Т.И. Правовое обеспечение информационной безопасности несовершеннолетних в условиях цифровой трансформации общества: дисс. ... кандидата юридических наук: 12.00.14 / Т.И. Сустина. – 2023 [Электронный ресурс]. – Режим доступа: https://www.dissercat.com/content/pravovoe-obespechenie-informatsionnoi-bezopasnosti-nesovershennoletnikh-v-usloviyakh-tsifrov (дата обращения: 15.01.2026). EDN CNXUWB

4. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 №436-ФЗ (ред. от 01.09.2024) // Официальный интернет-портал правовой информации [Электронный ресурс]. – Режим доступа: https://obrnadzor.gov.ru/wp-content/uploads/2024/12/federalnyj-zakon-№-436-fz.pdf (дата обращения: 15.01.2026).

5. Цветкова М.С. Информационная безопасность. Кибербезопасность: учебное пособие для 7–9 классов / М.С. Цветкова, И.Ю. Хлобыстова. – М.: Просвещение, 2023. – 64 с.

6. Цветкова М.С. Информационная безопасность. Безопасное поведение в сети Интернет: учебное пособие для 5–6 классов / М.С. Цветкова, Е.В. Якушина. – М.: Просвещение, 2024. – 96 с.-