«Формирование основ информационной безопасности у школьников на уроках информатики: от теории к жизненным ситуациям»

Автор: Григорова Елена Сергеевна,

учитель информатики МБОУ «Гимназия № 4» г.о. Самара

Современный школьник живёт в цифровой среде, которая для него так же естественна, как воздух. С первого класса — образовательные платформы, к пятому — активная жизнь в социальных сетях, к старшим классам — сложная цифровая идентичность. Но есть парадокс: будучи «цифровыми аборигенами», свободно обращающимися с гаджетами, дети зачастую остаются «цифровыми сиротами» в мире угроз, которые эта среда порождает. Фишинг, кибербуллинг, кража данных, манипуляции — это не абстрактные понятия, а реалии их ежедневного онлайн-бытия.

Задача школы — сформировать у подрастающего поколения не просто цифровую грамотность, а цифровой иммунитет. И здесь ключевая роль принадлежит нам, учителям информатики. Но как это сделать эффективно? Как уйти от формальных «уроков-страшилок» к реальным компетенциям? В своей практике я опираюсь на четыре ключевых принципа.

Первый принцип — возрастная адекватность. Тема информационной безопасности должна раскрываться постепенно, по спирали. В 7 классе мы говорим о безопасности устройства: вирусы, антивирусы, простые правила — не скачивай с сомнительных сайтов, не нажимай на яркие кнопки. Здесь работают метафоры: «пароль — это ключ от личного сейфа».

В 8-9 классах фокус смещается на безопасность личности в социуме: приватность в соцсетях, цифровой след, кибербуллинг, двухфакторная аутентификация. Подросток уже готов к разговору о причинно-следственных связях: «Что будет, если я выложу это фото?».

В старшей школе мы выходим на уровень понимания архитектуры цифрового мира: основы криптографии, правовые аспекты, экономика персональных данных.

Второй принцип — не запугать, а объяснить и научить. Страх — плохой учитель. Мы не говорим: «Интернет — это страшно». Мы говорим: «Интернет — это мощный инструмент. Давай научимся пользоваться им так, чтобы твои данные, твоя личность, твои устройства были под надёжным контролем». Это формирует уверенность и проактивную позицию.

Третий принцип — практико-ориентированность. Знания усваиваются прочно, когда они касаются жизни ученика «здесь и сейчас». Бесполезно читать лекцию о важности сложных паролей. Нужно провести практикум, где ребёнок создаст и проверит надёжность пароля для своего собственного аккаунта в игре или соцсети.

Изучая тему «Компьютерные сети», мы проводим практикум «Анатомия пароля» — дети через онлайн-сервисы проверяют стойкость паролей. Разбираем реальные *фишинговые письма*: ищем признаки подделки — незнакомые ссылки, грамматические ошибки, атмосферу

срочности и угрозы. И конечно, тема *кибербуллинга*. Через ролевые игры и кейсы мы отрабатываем алгоритмы действий: сохранить доказательства, заблокировать агрессора, обратиться к взрослым.

Четвёртый принцип — межпредметность и интеграция. Информационная безопасность лежит на пересечении дисциплин. С обществознанием и правом мы говорим о защите персональных данных, с психологией — о механизмах манипуляции, с математикой — об основах криптографии.

В 9 классе при изучении алгоритмизации мы делаем проект «Алгоритм верификации новости». Ребята создают блок-схему или пишут программу, которая задаёт череду проверочных вопросов: «Кто автор?», «Есть ли ссылки на первоисточники?», «Когда опубликовано?», «Что говорят другие источники?». Это учит не верить, а проверять.

В старшей школе, изучая базы данных, мы выходим на дискуссию о Big Data, таргетированной рекламе и ценности персональных данных. А на уроках программирования пишем простые программы, реализующие шифр Цезаря, — это даёт глубинное понимание принципов защиты информации.

Но важно понимать: усилия одного учителя, сколь бы искусны они ни были, ограничены без создания единой цифровой среды. Поэтому мы активно работаем с родителями и коллегами. *С родителями* проводим не лекции о «страшном интернете», а практикумы: «Цифровая гигиена в семье: правила без скандалов». Вместе настраиваем семейный контроль не как тотальную слежку, а как инструмент диалога о границах. Обсуждаем, что делать, если ребёнок столкнулся с травлей. *С педагогами* проводим консультации: как оценить достоверность источника для реферата, как модерировать конфликты в классных чатах.

И конечно, мы используем готовые ресурсы: «Урок цифры» с отличными тренажёрами, платформу «Изучи интернет — управляй им», материалы Лиги безопасного интернета.

Как мы оцениваем результаты? Уходим от тестов на воспроизведение терминов. Оцениваем продукт: созданный буклет для родителей, настройки приватности своего аккаунта с пояснениями, рефлексивное эссе «Что я изменил в своих цифровых привычках». Главное — не заученные правила, а реальные изменения в поведении.

Формирование культуры информационной безопасности — ***не частная задача учителя информатики, а стратегическая цель всей школы***. Мы должны воспитать поколение, которое будет воспринимать безопасность не как обременительное ограничение, а как естественную основу своей свободы и комфорта в цифровом мире. Поколение, способное не только пользоваться технологиями, но и управлять ими, защищая своё право на приватность, достоинство и интеллектуальную автономию. В этом — наша профессиональная и гражданская ответственность.