

Хмелев Сергей Геннадьевич

учитель

МБОУ «Синекинчерская ООШ им. М.Н. Юхмы»

д. Сине-Кинчеры, Чувашская Республика

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ В КУРСЕ ИНФОРМАТИКИ: ФОРМИРОВАНИЕ БЕЗОПАСНОГО ПОВЕДЕНИЯ ШКОЛЬНИКОВ В ЦИФРОВОЙ СРЕДЕ

***Аннотация:** в статье рассматриваются вопросы включения основ кибербезопасности в школьный курс информатики. Обосновывается актуальность формирования у обучающихся навыков безопасного поведения в цифровой среде. Описаны методы и приёмы преподавания темы, приведены примеры практических заданий, проанализированы результаты апробации в 7–9 классах. Особое внимание уделено интеграции теории с практикой: разбору реальных ситуаций, моделированию угроз, проектной деятельности. Представлена таблица схема этапов формирования кибербезопасности. Сделан вывод о необходимости системного подхода к обучению кибербезопасности на уроках информатики и во внеурочной деятельности.*

***Ключевые слова:** кибербезопасность, информатика, цифровая среда, безопасное поведение, парольная защита, фишинг, персональные данные, цифровая грамотность.*

Введение.

Стремительное развитие цифровых технологий привело к тому, что современные школьники проводят в интернете значительную часть времени. По данным исследований, более 80% подростков ежедневно пользуются социальными сетями, мессенджерами и онлайн-играми. При этом уровень их осведомлённости о киберугрозах остаётся недостаточным. Мошенничество, фишинг, утечка персональных данных, кибербуллинг – эти явления становятся частью повседневной жизни, и школа обязана реагировать на новые вызовы.

Предмет «Информатика» располагает наибольшим потенциалом для формирования основ кибербезопасности, поскольку именно в рамках этого курса изучаются принципы работы сетей, способы хранения и передачи информации, вопросы защиты данных. Однако практика показывает, что тема кибербезопасности часто рассматривается фрагментарно и не носит системного характера.

Цель статьи – обобщить методический опыт включения основ кибербезопасности в курс информатики основной школы.

Задачи:

- определить содержание темы «Кибербезопасность» в контексте школьного курса информатики;
- описать методы и приёмы преподавания;
- привести примеры практических заданий;
- проанализировать результаты апробации.

Основная часть.

1. Содержание темы «Кибербезопасность» в школьном курсе.

Тема кибербезопасности может быть интегрирована в различные разделы курса информатики:

- «Информация и информационные процессы» – понятие конфиденциальности, ценности информации;
- «Компьютер как универсальное устройство» – защита устройства, антивирусные программы;
- «Обработка графической информации» – безопасное использование изображений, авторское право;
- «Коммуникационные технологии» – безопасная работа в сети, защита персональных данных.

Ключевые содержательные линии:

- защита персональных данных;
- парольная защита и двухфакторная аутентификация;
- распознавание фишинга и мошеннических схем;
- безопасное поведение в социальных сетях;

- кибербуллинг и его профилактика;
- авторское право и цифровая этика.

2. Методы и приёмы преподавания.

Эффективными методами обучения кибербезопасности являются:

- *кейс-метод* – разбор реальных ситуаций (например, «Вам пришло письмо от имени банка с просьбой подтвердить данные»);
- *моделирование* – создание учебных фишинговых писем и их анализ;
- *ролевые игры* – «Безопасный чат», «Что делать, если взломали аккаунт»;
- *проектная деятельность* – разработка памяток, буклетов, видеороликов о кибербезопасности;
- *практические работы* – проверка надёжности паролей, настройка приватности в социальных сетях.

Особое значение имеет принцип «равный – равному»: старшеклассники могут готовить занятия для младших школьников, что повышает и их собственную мотивацию.

Формирование кибербезопасности целесообразно выстраивать поэтапно, с учётом возрастных особенностей обучающихся. Этапы этой работы представлены в таблице 1.

Таблица 1

Этапы формирования кибербезопасности школьников

Этап	Классы	Содержание	Формы работы
1. Знакомство	5–6	Понятие безопасности в сети, правила поведения	Беседы, игры, просмотр видеороликов
2. Освоение базовых правил	7–8	Пароли, персональные данные, фишинг	Практические работы, кейсы
3. Углубление	9	Кибербуллинг, социальная инженерия, авторское право	Ролевые игры, проекты
4. Практика	8–9	Разработка памяток, обучение младших	Проектная деятельность, наставничество
5. Рефлексия	все	Анализ собственного поведения в сети	Анкетирование, портфолио

3. Примеры практических заданий.

Задание 1. «Проверка надёжности пароля».

Обучающимся предлагается оценить пароли по критериям: длина, наличие цифр, букв разного регистра, специальных символов. Используются онлайн-сервисы проверки надёжности.

Задание 2. «Фишинг или нет?».

Учащиеся анализируют несколько писем и определяют, какие из них являются мошенническими. Указывают признаки: подозрительный адрес отправителя, ошибки в тексте, просьба перейти по ссылке.

Задание 3. «Настройка приватности».

Практическая работа в социальной сети (на учебном аккаунте): настройка видимости профиля, ограничение доступа к личным данным.

Задание 4. «Кибербезопасность в моей жизни».

Мини-проект: анализ собственных привычек в сети, разработка личной стратегии защиты.

4. Результаты апробации.

Апробация методики проводилась в МБОУ «Синекинчерская ООШ им.М.Н.Юхмы» в 7–9 классах в течение 2025–2026 учебного года. Диагностика включала анкетирование до и после обучения, наблюдение, анализ практических работ.

Результаты:

- доля обучающихся, знающих основные виды киберугроз, выросла с 62% до 89%;
- количество учащихся, использующих сложные пароли, увеличилось с 45% до 72%;
- 82% школьников отметили, что стали более внимательно относиться к личным данным в сети;
- повысился интерес к теме: 45% выбрали кибербезопасность темой итогового проекта.

Полученные данные свидетельствуют о положительном влиянии системного подхода к изучению кибербезопасности.

Заключение.

Формирование основ кибербезопасности является важной задачей современного школьного образования. Курс информатики предоставляет широкие возможности для решения этой задачи. Системный подход, сочетающий теоретические сведения с практическими заданиями, разбором реальных ситуаций и проектной деятельностью, позволяет сформировать у обучающихся устойчивые навыки безопасного поведения в цифровой среде. Перспективой дальнейшей работы является разработка сквозной программы по кибербезопасности для 5–11 классов и активное включение родителей в образовательный процесс.

Список литературы

1. Босова, Л. Л. Информатика. 7 класс : учебник / Л. Л. Босова, А. Ю. Босова. – Москва : БИНОМ. Лаборатория знаний, 2020. – 240 с.
2. О персональных данных : Федеральный закон от 27.07.2006 №152-ФЗ. – URL: <http://www.consultant.ru> (дата обращения: 20.10.2026). – Текст : электронный.