**77017900679**

**770816301456**

****

**МУХАМЕДЖАНОВ Руслан Адильбекович,**

**Т.Рысқұлов атындағы орта мектебінің информатика пәні мұғалімі.**

**Алматы облысы, Еңбекшіқазақ ауданы**

**СТАТЬЯ «КИБЕРБЕЗОПАСНОСТЬ: ОБУЧЕНИЕ ШКОЛЬНИКОВ БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ ИНТЕРНЕТА»**

**Введение**

Современные школьники проводят значительное время в интернете, используя его для учебы, общения и развлечений. Однако цифровая среда несет в себе множество рисков: онлайн-мошенничество, нарушение конфиденциальности, дезинформация. Важно не только предостерегать детей от угроз, но и обучать их безопасному использованию интернет-ресурсов.

Данное пособие предназначено для педагогов и родителей. В нем собраны методики, практические задания и рекомендации, направленные на формирование ответственного цифрового поведения школьников.

**ГЛАВА 1. ОСНОВЫ БЕЗОПАСНОСТИ В СЕТИ**

**1.1. Основные принципы цифровой безопасности**

* Управление личными данными в сети;
* Осознание рисков кибератак;
* Использование надежных паролей;
* Ответственное поведение в соцсетях.

**1.2. Распространенные интернет-угрозы**

* **Вирусы и вредоносное ПО** – могут повредить устройство и украсть данные.
* **Фишинговые атаки** – мошенники маскируются под доверенные сервисы.
* **Кибербуллинг** – агрессия и запугивание в сети.
* **Социальная инженерия** – манипуляции с целью обмана.

**ГЛАВА 2. КОНФИДЕНЦИАЛЬНОСТЬ ЛИЧНЫХ ДАННЫХ**

**2.1. Какие данные следует защищать?**

* ФИО, адрес, телефон, данные банковских карт.
* Логины и пароли от онлайн-аккаунтов.
* Фотографии, видео, персональные сообщения.

**2.2. Надежная аутентификация**

* Пароли должны быть длинными и сложными.
* Использование двухфакторной аутентификации (2FA).
* Регулярное обновление паролей.

**ГЛАВА 3. БЕЗОПАСНОЕ ОНЛАЙН-ОБЩЕНИЕ**

**3.1. Как избежать интернет-обмана**

* Проверять подлинность сообщений и сайтов.
* Не передавать личные данные незнакомцам.
* Игнорировать подозрительные ссылки.

**3.2. Как реагировать на онлайн-угрозы**

* Сохранять доказательства кибербуллинга.
* Блокировать агрессоров в соцсетях.
* Сообщать о проблемах взрослым или в правоохранительные органы.

**ГЛАВА 4. КУЛЬТУРА ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ**

**4.1. Осознанное использование интернета**

* Цифровой след: информация, которую оставляет пользователь.
* Возможные риски публикации личных данных.
* Как настроить конфиденциальность аккаунтов.

**4.2. Проверка достоверности информации**

* Анализ источников и перекрестная проверка фактов.
* Как выявить фейки и пропаганду.
* Информационная гигиена: не распространять непроверенные данные.

**4.3. Правила общения в интернете**

* Вежливость и уважение собеседников.
* Безопасное поведение в чатах и комментариях.
* Как избегать конфликтов и провокаций.

**ГЛАВА 5. ПРАКТИЧЕСКИЕ ЗАДАНИЯ**

**5.1. Интерактивные уроки по интернет-безопасности**

* Викторины о киберугрозах.
* Анализ мошеннических сообщений.
* Настройки безопасности профиля.

**5.2. Разбор реальных случаев**

* Что делать при утечке личных данных?
* Как противостоять кибербуллингу?
* Как не попасть на уловки мошенников?

**5.3. Создание правил ответственного поведения**

* Регулирование времени в интернете.
* Развитие критического мышления.
* Коллективное обсуждение кибербезопасности в классе.

**Заключение**

Разработанный материал может быть использован на уроках информатики, классных часах, внеклассных занятиях и родительских собраниях. Он также может стать основой для создания школьных программ по кибербезопасности, онлайн-курсов и интерактивных тренингов.

Формирование цифровой культуры у школьников – совместная задача педагогов, родителей и самих детей. Чем раньше учащиеся освоят правила безопасного поведения в интернете, тем увереннее и безопаснее они смогут использовать современные технологии в своей жизни.

Обучая детей кибербезопасности сегодня, мы создаем цифрово-грамотное общество будущего!

**Список литературы**

1. Закон РК «О персональных данных».
2. Беляков С.А. «Интернет-безопасность».
3. Национальный центр информационной безопасности РК – [www.ncsc.kz](http://www.ncsc.kz/)