МБУ «Новолеушковская сельская библиотека им.И.И. Никонова»

Безопасность в сети Интернет

Подготовила: зав.сектором по работе с юношеством Остапенко Т.Н.

Интернет – это интересный и увлекательный мир, который позволяет узнавать много интересного, общаться с людьми в разных концах света, играть в интересные игры и делиться с другими своими мыслями и увлечениями. Интернет экономит время на подготовку к занятиям, делает процесс учёбы более интересным.

В современном мире, дети выходят в интернет раньше, чем учатся писать. По данным UNICEF, цифровая среда для них уже не «виртуальная зона», а естественное продолжение повседневной жизни.

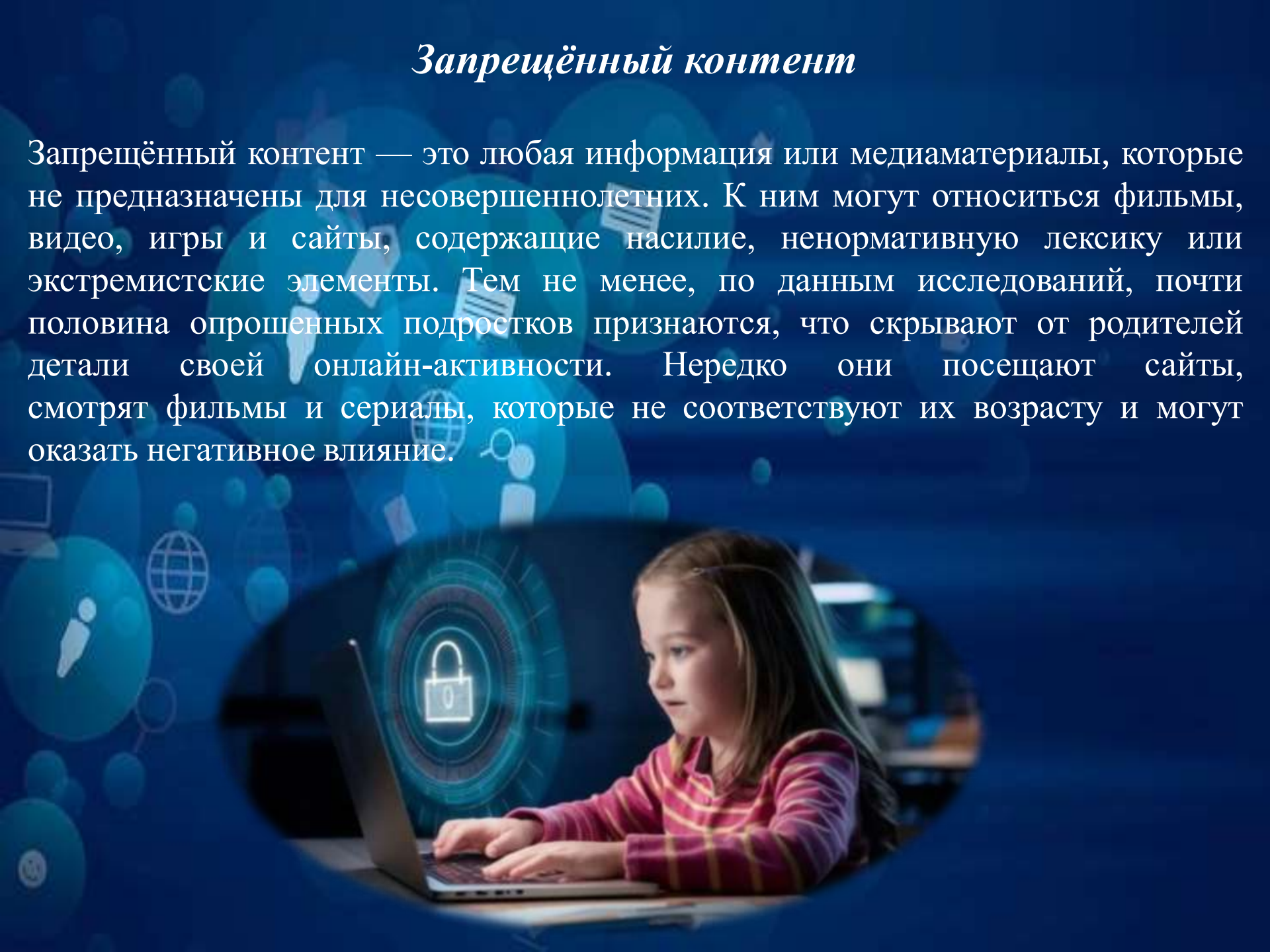
На данный момент существует много типов угроз для детей и подростков в интернете. Рассмотрим некоторые из них.

Кибербуллинг

Кибербуллинг, или травля в интернете, представляет собой целенаправленные угрозы, оскорбления и другие формы агрессивного поведения со стороны одного или нескольких пользователей. Такие действия, как правило, направлены на причинение эмоционального вреда, запугивание или социальное изгнание жертвы. В отличие от традиционной формы травли, кибербуллинг может происходить в любое время суток, причём агрессоры зачастую остаются анонимными, что делает ситуацию особенно сложной для пострадавшего.

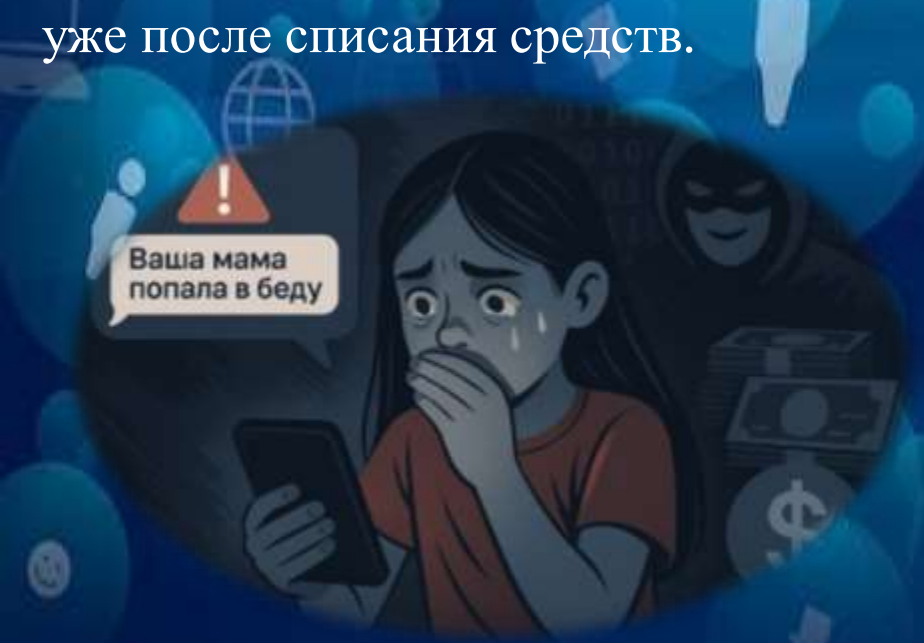
Запрещённый контент

Запрещённый контент — это любая информация или медиаматериалы, которые не предназначены для несовершеннолетних. К ним могут относиться фильмы, видео, игры и сайты, содержащие насилие, ненормативную лексику или экстремистские элементы. Тем не менее, по данным исследований, почти половина опрошенных подростков признаются, что скрывают от родителей детали своей онлайн-активности. Нередко они посещают сайты, смотрят фильмы и сериалы, которые не соответствуют их возрасту и могут оказать негативное влияние.



Мошенничество

Мошенники часто используют доверчивость детей, обманывая их и завладевая деньгами через бесплатные приложения, тесты в социальных сетях и подозрительные почтовые рассылки. Они заманивают юных пользователей, предлагая перейти по ссылке, ввести номер телефона или данные банковской карты родителей. Один из распространённых способов обмана — это онлайн-игры, где дети могут приобретать за реальные деньги дополнительные предметы: снаряжение, оружие или игровые способности. При этом стоимость таких покупок может быть значительной, а родители узнают о произошедшем уже после списания средств.



Вредоносное ПО

Вредоносное программное обеспечение, или вредоносное ПО, — это программы, специально созданные для нарушения работы устройств и получения несанкционированного доступа к данным. Заражение может происходить через подозрительные ссылки, вложения в электронные письма или небезопасные сайты. Последствия такого заражения могут быть серьёзными: от кражи конфиденциальной информации, такой как пароли и номера банковских карт, до утраты личных файлов и фотографий.

Доступ к личной информации

Даже если смартфон или компьютер подключён к домашней сети, личная информация, которую дети оставляют или ищут в интернете — особенно в социальных сетях — может быть доступна не только родителям, но и посторонним людям. Всё, что публикуется в веб-пространстве, может быть найдено, сохранено и использовано без ведома пользователя.

Поэтому ***кибербезопасность*** становится всё более важной темой. С развитием информационных технологий и повсеместным распространением интернета дети всё чаще оказываются уязвимыми перед различными угрозами виртуального мира. В таких условиях особенно важно научить их осознанному и ответственному поведению в онлайн-среде — с пониманием рисков и уважением к личным границам, как своими, так и чужим.

Как защитить ребёнка в интернете?

- НЕ использовать личную информацию в названиях. Многие дети используют свое имя, фамилию и дату рождения при установке названия аккаунтов, адресов электронной почты. Это помогает преступникам воровать и использовать персональные данные, подбирать пароли, отслеживать детей.
- НЕ выкладывать в сеть фото и видео с личными данными. Получая паспорт и другие документы, многие дети хвастаются этим в соцсетях. Они могут случайно сделать кадр или видео, на котором будут видны документы. Поэтому каждую публикацию нужно проверять.
- НЕ открывать подозрительные ссылки, не скачивать странные файлы. И это касается не только загрузки развлекательного контента. Важно рассказать ребенку о провокациях мошенников: они могут отправлять ссылки и файлы в личных сообщениях, или при помощи рекламы и оскорблений завлекать ребенка на свою страницу: никаких данных о человеке в аккаунте нет, но есть ссылка, по которой и переходит любопытный ребенок.

Ссылки и файлы используют для кражи данных, взлома социальных сетей и банковских приложений, внедрения вирусов или программ слежения на компьютер и смартфон.

- НЕ давать никому свой пароль. Даже близким друзьям. Приведите ребенку аналогию с ключами от квартиры родителей: вы ведь не допустите, чтобы чужой человек мог в любое время зайти в дом? Пароли от соцсетей ребенка могут знать только самые близкие родственники.

При этом стоит обсудить правила личного пространства. Например, до определенного возраста (чаще всего до 14-15 лет) родители обязательно должны иметь доступ к аккаунтам ребенка.

- Настроить многофакторную аутентификацию. Помогите ребенку установить сложную защиту в социальных сетях и приложениях (особенно банковских, если они есть). Это вход в систему в несколько шагов: ввод пароля, проверочный код в смс или электронной почте.
- НЕ хранить в смартфоне\ноутбуке\компьютере документы и фотографии с ними. Личные устройства всегда могут взломать. Поэтому ребенок должен следить за тем, что он хранит на своих гаджетах.

Как защитить компьютер ребёнка в киберпространстве

1) **Создайте отдельную учётную запись без прав администратора** — это позволит ограничить доступ к установке программ и изменению важных настроек системы.
2) **Регулярно обновляйте операционную систему** — своевременные обновления помогают устранить уязвимости, которые могут быть использованы злоумышленниками.
3) **Используйте только лицензионное программное обеспечение** — оно проходит проверку на безопасность и снижает риск заражения вредоносными файлами.
4) **Установите антивирусное программное обеспечение** и регулярно проводите проверку системы, чтобы выявлять и устранять потенциальные угрозы.
5) **Активируйте функции родительского контроля** через настройки операционной системы или специализированные приложения — это поможет ограничить доступ к нежелательному контенту и отслеживать онлайн-активность ребёнка.

Как защитить смартфон ребёнка от киберугроз

1) Установите ПИН-код на сим-карту устройства, чтобы предотвратить её использование на других устройствах.
2) Воспользуйтесь возможностью биометрической аутентификации, такой как распознавание отпечатка пальца или лица, чтобы надёжно защитить смартфон и его содержимое.
3) Активируйте службы геолокации, чтобы иметь возможность контролировать местонахождение устройства ребёнка.
4) Настройте функции родительского контроля с помощью операционной системы или отдельных приложений.

Использованные источники:

- https://dzen.ru/a/ZfrAZwyri0zEhGe9
- https://nsportal.ru/shkola/raznoe/library/2018/03/01/bezopasnost-detey-v-seti-internet
- https://skillbox.ru/media/code/pravila-bezopasnosti-detej-v-internete/
- https://media.foxford.ru/articles/zashhita-rebenka-v-internete
- https://www.itechnewsonline.com/wp-content/uploads/2022/03/istock-1265582618.jpg
- https://images.prismic.io/kidskey/18f13d0f-fb7f-4083-b212-fe62157b9b61_kiber4.jpg?auto=compress,format
- https://avatars.mds.yandex.net/get-images-cbir/1747226/L3Z4ILI_bk7c9K7pWl8oRA9763/ocr
- https://png.pngtree.com/thumb_back/fh260/background/20241016/pngtree-a-stark-contrast-of-light-and-dark-colors-symbolizing-the-hidden-image_16401206.jpg
- https://static59.tgcnt.ru/posts/_0/4e/4ecbf5d73b7d90a752f81e38c84a6ec8.jpg
- https://avatars.mds.yandex.net/i?id=ad932b61df38d11b9b66de14691338344a370821-5235855-images-thumbs&n=13
- https://images.prismic.io/kidskey/18f13d0f-fb7f-4083-b212-fe62157b9b61_kiber4.jpg?auto=compress,format
- https://avatars.mds.yandex.net/i?id=91d656c73141b392e8fa435f55d01783_l-4417086-images-thumbs&n=13
- https://region.center/source/Ivanovo/2025/01/22/vjityybrb.jpg
- https://region.center/source/Ivanovo/2025/01/22/vjityybrb.jpg
- https://region.center/source/Ivanovo/2025/01/22/vjityybrb.jpg